Titolo dello studio	Studio CARE – Epidemiologia del Tumore al Seno Triplo Negativo in Italia: Caratterizzazione dei Pazienti e dei Modelli di Trattamento
Promotore	MSD Italia S.r.l. Via Vitorchiano, 151 00189 Rome Italy
Centro di Sperimentazione	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Principal Investigator	Dott. Michelino De Laurentiis S.C. Oncologia Clinica Sperimentale di Senologia Istituto Nazionale Tumori IRCCS Fondazione G. Pascale
Tipo di studio e fase	Studio multicentrico, osservazionale, retrospettivo.
Parere del Comitato Etico	Parere favorevole del 21.12.2022
DPO/RPD	Ing. Alessandro Manzoni

	Nome e Cognome	Ruolo	Firma	Data
	Roberta Fusco	Ingegnere Biomedico	[redacted]	27/08/2025
Revisione	Gianfranco De Feo	Quality Assurance	[redacted]	27/08/2025
Approvazione	Maurizio Di Mauro	Titolare del trattamento dati	Firmato digitalmente da: Maurizio Di Mauro Ruolo: DIRETTORE GENERALE Organizzazione: IRCCS FONDAZIONE G.PASCALE/00911350635 Data: 12/09/2025 12:05:59	
	Alessandro Manzoni	DPO	Firmato digitalmente da: Alessandro Manzoni Ruolo: DIRIGENTE INGEGNERE Organizzazione: IRCCS FONDAZIONE G. PASCALE/00911350635 Data: 11/09/2025 13:20:33	
	Michelino De Laurentiis	Principal Investigator Centro Satellite	[redacted]	27/08/2025
	Gianfranco De Feo	Quality Assurance	[redacted]	27/08/2025

Tracking delle modifiche

N° Rev.	Data	Motivo della modifica	Paragrafi
1.1	10.07.2025	Prima emissione	TUTTI

Storico della rivalutazione

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

	Data prevista	Data effettiva	Firma
Rivalutazione a cura del QA			

Tabella dei Contenuti

1. Stima del rischio e pre-assessment

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

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

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

2. Quadro normativo

Regolamento (UE) 679/2016 (GDPR);
D.lgs. 196/2003 e s.m.i. per effetto del D.lgs. 101/2018;
Articolo 29 Working Party (2017), Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" in base alle disposizioni contenute nel Regolamento (UE) 679/2016;
Provvedimento 146/2019 del Garante per la protezione dei dati personali.
Provvedimento 298/2024 del Garante per la protezione dei dati personali.

3. Contesto

3.1 Titolare e Responsabile della Protezione dei Dati

Titolare dei trattamenti dei Suoi dati personali effettuati presso il Centro di Sperimentazione Istituto Nazionale dei Tumori IRCCS di Napoli Fondazione G. Pascale è il Legale Rappresentante e il dott. Michelino De Laurentiis in qualità di Principal

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

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

- Altro

Non applicabile

RICHIESTA DEL PARERE DEGLI INTERESSATI RELATIVAMENTE ALLA DPIA

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

MOTIVAZIONE DELLA MANCATA RICHIESTA DEL PARERE ALLA DPIA DEGLI INTERESSATI

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

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

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

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Il trattamento oggetto della presente valutazione riguarda la raccolta, l'elaborazione e la trasmissione di dati personali relativi a pazienti oncologici affetti da carcinoma mammario triplo negativo (TNBC), nell'ambito dello studio osservazionale non interventistico CARE (protocollo NIS102061), promosso da MSD Italia S.r.l.
In particolare, il trattamento consiste in:

- Estrazione retrospettiva dei dati clinici dalla documentazione sanitaria archiviata presso l'Istituto.
- Registrazione elettronica dei dati pseudonimizzati nel sistema eCRF fornito dallo sponsor e gestito dalla CRO.
- Conservazione dei dati pseudonimizzati presso il centro fino alla chiusura dello studio.
- Trasmissione protetta dei dati pseudonimizzati ai rappresentanti dello sponsor per finalità di analisi epidemiologica, economica e gestionale.

Il trattamento include anche:

- Dati relativi a soggetti deceduti o non contattabili, in conformità all'art. 110 del Codice Privacy e al Provvedimento n. 298/2024 del Garante per la Protezione dei Dati Personali, previa autorizzazione del Comitato Etico e pubblicazione dell'informativa ai sensi dell'art. 14 GDPR.
- Dati anagrafici e professionali degli operatori sanitari coinvolti nel progetto (es. Principal Investigator, Data Manager), ai fini della gestione amministrativa dello studio.

Il trattamento è limitato esclusivamente ai dati pertinenti e necessari per il raggiungimento degli obiettivi dello studio ed è condotto in conformità alle normative vigenti in materia di protezione dei dati personali (Regolamento UE 2016/679 - GDPR e D.lgs. 196/2003, come modificato).

3.3.2 Quali sono le responsabilità connesse al trattamento?

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

1. Titolare del Trattamento (Data Controller)

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

Responsabilità:

- Determinare le Finalità e i Mezzi del Trattamento: Decidere come e perché i dati personali devono essere trattati.
- Garantire la Conformità al GDPR: Assicurarsi che tutte le attività di trattamento siano conformi alle disposizioni del Regolamento Generale sulla Protezione dei Dati (GDPR).
- Informativa sulla Privacy: Fornire informazioni chiare e trasparenti agli interessati riguardo al trattamento dei loro dati.
- Consenso Informato: Ottenere il consenso informato dai partecipanti, assicurando che siano a conoscenza di come saranno utilizzati i loro dati.
- Valutazione dell'Impatto sulla Protezione dei Dati (DPIA): Condurre una DPIA per identificare e mitigare i rischi associati al trattamento.
- Gestione dei Diritti degli Interessati: Assicurarsi che gli interessati possano esercitare i loro diritti (accesso, rettifica, cancellazione, ecc.).
- Sicurezza dei Dati: Implementare misure tecniche e organizzative adeguate per proteggere i dati personali.

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

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

Responsabilità:

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

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

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

3. Preposto autorizzato al trattamento

Per codesto progetto, questo ruolo è stato delegato per il Centro di Sperimentazione per il dott. Michelino De Laurentiis.

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.

4. Personale Coinvolto nel Trattamento

Il personale che tratta i dati personali deve essere adeguatamente formato e consapevole delle proprie responsabilità.

Responsabilità:

Riservatezza: Mantenere la riservatezza delle informazioni personali trattate.

Conformità alle Politiche Aziendali: Seguire le politiche e le procedure aziendali relative alla protezione dei dati.
Segnalazione di Incidenti: Segnalare tempestivamente eventuali incidenti di sicurezza o violazioni dei dati.

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

Nel contesto dello studio osservazionale CARE (NIS102061), le responsabilità connesse al trattamento dei dati personali presso l'Istituto Nazionale dei Tumori IRCCS "Fondazione G. Pascale" di Napoli sono così ripartite:

Centro sperimentale – Titolare autonomo del trattamento
L'Istituto agisce in qualità di **titolare autonomo del trattamento** per quanto riguarda:
- L'identificazione e la selezione dei pazienti eleggibili.
- La raccolta dei dati clinici dalle cartelle sanitarie.
- La pseudonimizzazione dei dati prima dell'inserimento nell'eCRF.
- La conservazione locale dei dati secondo le normative sanitarie vigenti.
- L'adozione di misure tecniche e organizzative adeguate a proteggere i dati (es. gestione degli accessi, tracciamento attività, formazione del personale).

Sponsor – MSD Italia S.r.l.
Lo sponsor è **titolare del trattamento** dei dati una volta ricevuti in forma pseudonimizzata.
È responsabile della:
- Definizione delle finalità e modalità del trattamento.
- Analisi statistica ed epidemiologica dei dati.
- Custodia dei dati presso le proprie infrastrutture sicure.
- Redazione e pubblicazione della DPIA a livello nazionale.
- Pubblicazione dell'informativa ex art. 14 GDPR per soggetti deceduti/non contattabili.

CRO – PHIDEALIVE s.r.l
La CRO agisce **in qualità di responsabile del trattamento** per conto dello sponsor. Le sue responsabilità includono:
- La gestione tecnica della piattaforma eCRF e dei flussi di dati.
- Il supporto operativo e formativo ai centri partecipanti.
- La gestione dei monitoraggi e dei controlli di qualità.
- Il rispetto degli obblighi contrattuali e normativi relativi alla sicurezza e alla riservatezza dei dati.

3.3.3 Ci sono standard applicabili al trattamento?

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

1. Regolamento Generale sulla Protezione dei Dati (GDPR)
Il GDPR è il principale standard legale per la protezione dei dati personali nell'Unione Europea. Ecco alcuni dei requisiti chiave:
Principi del Trattamento dei Dati: I dati personali devono essere trattati in modo lecito, corretto e trasparente; raccolti per finalità determinate, esplicite e legittime; adeguati, pertinenti e limitati a quanto necessario; esatti e, se necessario, aggiornati; conservati in una forma che consenta l'identificazione degli interessati per un periodo non superiore al necessario; trattati in modo da garantire la sicurezza adeguata dei dati.
Diritti degli Interessati: Gli interessati hanno il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e opposizione al trattamento.
Valutazione d'Impatto sulla Protezione dei Dati (DPIA): Necessaria quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
Sicurezza dei Dati: Obbligo di implementare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.
Notifica di Violazione dei Dati: Obbligo di notificare le violazioni dei dati personali all'autorità di controllo entro 72 ore e, in certi casi, agli interessati.

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

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

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

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

6. Standard di sicurezza e qualità applicati
- Good Clinical Practice (ICH-GCP E6 R3).
- Good Pharmacoepidemiology Practices (GPP).
- ISO/IEC 27001 per la gestione della sicurezza delle informazioni.
- ISO/IEC 27002, 27017, 27018, ove applicabili, per la protezione dei dati in ambienti cloud e sanitari.
- 21 CFR Part 11 (FDA, per sistemi elettronici conformi).
- OSSTMM e OWASP per la sicurezza delle applicazioni web (es. piattaforma eCRF).
- NIST SP 800-115 per il penetration testing e la gestione dei rischi IT.
- Standard di pseudonimizzazione e crittografia riconosciuti a livello europeo.

3.4 Dati, processi e risorse di supporto

3.4.1 Quali sono i dati trattati?

Nel contesto dello studio osservazionale retrospettivo CARE (protocollo NIS102061), il trattamento riguarda le seguenti categorie di dati personali, raccolti a partire dalle cartelle cliniche dei pazienti trattati presso l'Istituto Nazionale dei Tumori IRCCS "Fondazione G. Pascale" di Napoli:

- Dati anagrafici e demografici (pseudonimizzati):
  - Anno e mese di nascita
  - Sesso
  - Altezza, peso
  - Comorbidità

- Dati sanitari**:**
  - Data della diagnosi di tumore mammario triplo negativo (TNBC)
  - Caratteristiche istologiche e biomolecolari del tumore (ER, PgR, HER2, PD-L1, TILs, AR)
  - Stadio clinico (secondo classificazione AJCC TNM)
  - Risultati di test genetici (BRCA1/2, multigene panel)
  - Tipologia e date di interventi chirurgici (conservativa, mastectomia, linfonodi)
  - Dettagli sul trattamento sistemico (neoadiuvante, adiuvante) e radioterapia
  - Risposta patologica (pCR)
  - Eventuale recidiva, progressione, sopravvivenza e stato vitale
  - Date e modalità di esiti (morte, recidiva, follow-up)
  - Utilizzo di risorse sanitarie: ricoveri, visite, esami, trattamenti

- Dati degli operatori sanitari coinvolti (HCP):
  Nome, cognome, qualifica professionale, contatti istituzionali
  (utilizzati esclusivamente per la gestione dello studio e le comunicazioni con sponsor e CRO)
- Dati di pazienti deceduti o non rintracciabili:
  - Trattati nel rispetto dell'art. 110 del Codice Privacy e secondo il principio di minimizzazione.
  - Nessun dato identificativo viene comunicato allo sponsor o alla CRO.
  - Viene applicata pseudonimizzazione, e l'elenco dei codici è custodito solo localmente.

Tutti i dati sono pseudonimizzati prima dell'inserimento nel sistema elettronico (eCRF) e gestiti secondo rigide misure di sicurezza. Nessun dato direttamente identificativo (es. nome, codice fiscale, indirizzo) viene trasferito o condiviso con lo sponsor o altri soggetti esterni.

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

1. Identificazione e selezione
   - L'investigatore individua i pazienti eleggibili (diagnosi TNBC tra gennaio 2018 e dicembre 2021) rivedendo cartelle cliniche in archivio.

2. Pseudonimizzazione
   - A livello locale, prima di qualsiasi inserimento, i dati vengono codificati con un ID non direttamente riconducibile al paziente.
   - La chiave di decodifica rimane solo nel centro, mai trasferita.

3. Raccolta e inserimento dati
   - I dati pseudonimizzati vengono inseriti dagli operatori autorizzati nel sistema elettronico eCRF, gestito dalla CRO.
   - Solo il personale con accesso autenticato può operare nel sistema.

4. Verifica e monitoraggio qualità
   - La CRO esegue controlli sistematici di qualità (monitoring, controlli di coerenza e formazione continua del personale).

5. Conservazione locale
   - L'Istituto conserva i dati in formato pseudonimizzato secondo normative sanitarie vigenti, con misure di sicurezza (accesso controllato, backup, logging).

6. Trasmissione allo sponsor
   - Al termine del periodo operativo, la CRO trasferisce allo sponsor (MSD) i dati pseudonimizzati in modalità sicura e protetta, senza includere informazioni identificative.

7. Elaborazione analitica e studio

- Lo sponsor utilizza i dati per analisi epidemiologiche, economiche e statistiche, in conformità con lo scopo autorizzato dal protocollo.

8. Conservazione centralizzata dello sponsor
   - I dati sono conservati nelle infrastrutture MSD in ambiente sicuro UE, conformi agli standard e retretti secondo il piano di retention (5 anni) e poi cancellati.

9. Distruzione finale
   - Al termine della conservazione prevista, i dati vengono eliminati sia nei sistemi dello sponsor che, in accordo con le policy, sul modello GPP.

10. Accesso autorizzato
    - Il personale coinvolto (sponsor, CRO, monitor, staff del centro) può consultare i dati solo per necessità legate allo studio, con accesso tracciato, autenticato e confinato alla durata autorizzata del progetto.

3.4.3 Quali sono le risorse di supporto ai dati?

Il trattamento dei dati personali nell'ambito dello studio CARE (NIS102061) è supportato da un insieme integrato di risorse tecniche, organizzative e umane, selezionate e gestite per garantire sicurezza, integrità e riservatezza dei dati in tutte le fasi del ciclo di vita.

1. Risorse tecnologiche (hardware/software)
   - Piattaforma eCRF elettronica validata, conforme a:
     - *GCP (Good Clinical Practice)*
     - *21 CFR Part 11* (standard FDA per sistemi elettronici)
   - Infrastruttura cloud-based o server dedicato, localizzata in Europa, dotata di:
     - Sistemi di accesso sicuro (username/password con lockout policy)
     - Connessioni cifrate (HTTPS/TLS)
     - Logging, auditing e tracciabilità degli accessi
     - Backup periodici su supporti criptati
     - Piano di disaster recovery
2. Risorse umane e organizzative
   - Personale clinico e amministrativo dell'Istituto, formato sul protocollo e sulla normativa privacy.
   - Referente privacy locale e Responsabile IT per il supporto operativo e la sorveglianza delle misure interne.
   - Data Protection Officer (DPO) dell'ente, coinvolto nella valutazione e nel monitoraggio del trattamento.
   - CRO, incaricata dal promotore per la gestione tecnica e il monitoraggio dei dati.
   - Sponsor (MSD Italia S.r.l.), che riceve solo dati pseudonimizzati, conserva e analizza i dati tramite infrastrutture interne sicure.
3. Documentazione e strumenti di governance
- Data Management Plan (DMP)
- Manuale utente eCRF
- Piano di formazione per lo staff
- Accordi contrattuali con clausole privacy e sicurezza

- DPIA nazionale e locale
- Registro delle attività di trattamento

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

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

4. Valutazione di necessità e proporzionalità del trattamento

4.1 Proporzionalità e necessità

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

Gli scopi del trattamento dei dati personali nell'ambito dello studio CARE (NIS102061) sono specifici, espliciti e legittimi, in conformità all'art. 5(1)(b) del GDPR.

Lo studio ha finalità scientifiche, epidemiologiche e sanitarie chiaramente definite nel protocollo approvato dal Comitato Etico e dal promotore. In particolare, gli obiettivi del trattamento includono:

- Analizzare le caratteristiche cliniche, demografiche e biologiche dei pazienti con carcinoma mammario triplo negativo (TNBC) diagnosticati tra il 2018 e il 2021.
- Valutare i percorsi terapeutici reali (real-world) e l'uso delle risorse sanitarie nel trattamento precoce del TNBC.
- Stimare gli esiti clinici (recidiva, risposta patologica, sopravvivenza).
- Analizzare l'impatto economico per il Servizio Sanitario Nazionale.
- Verificare l'accesso e l'uso dei test genetici e molecolari.
- Fornire evidenze utili a orientare pratiche cliniche, linee guida e politiche sanitarie.

Il trattamento è giustificato da motivazioni di interesse pubblico nel settore della salute pubblica e dalla finalità di ricerca scientifica in ambito medico, ai sensi dell'art. 9(2)(j) del GDPR e dell'art. 110 del Codice Privacy italiano.

Inoltre, tutti i trattamenti sono documentati nel protocollo di studio e nella valutazione d'impatto, e rispettano i principi di minimizzazione, trasparenza e responsabilizzazione (accountability).

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

Il trattamento dei dati personali effettuato nell'ambito dello studio osservazionale CARE (NIS102061) presso l'Istituto Nazionale dei Tumori IRCCS "Fondazione G. Pascale" di Napoli è lecito ai sensi del Regolamento (UE) 2016/679 (GDPR) e della normativa nazionale (D.lgs. 196/2003 e successive modificazioni), sulla base delle seguenti disposizioni:

Per soggetti viventi:

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

Per soggetti deceduti o non rintracciabili:

- Art. 110 del D.lgs. 196/2003 (Codice Privacy) – *Ricerca medica con dati di soggetti non contattabili/deceduti*:
  Il trattamento è consentito in presenza di:
  - Impossibilità pratica di informare l'interessato.
  - Parere favorevole del Comitato Etico.
  - Pubblicazione dell'informativa ex art. 14 GDPR (sito web istituzionale).
  - Rispetto delle misure previste dal Provvedimento n. 298/2024 del Garante Privacy.
- Art. 9(2)(j) GDPR – *Trattamento per fini di ricerca scientifica nel rispetto delle garanzie*:
  Il trattamento è legittimo in quanto finalizzato alla ricerca scientifica in ambito sanitario, accompagnato da misure appropriate per salvaguardare i diritti fondamentali degli interessati (es. pseudonimizzazione, limitazione dell'accesso, minimizzazione dei dati).

Per dati degli operatori sanitari (personale HCP):

- Art. 6(1)(b) GDPR – *Esecuzione di un contratto o misure precontrattuali*:
  Il trattamento è necessario per la gestione dello studio clinico e degli obblighi correlati alla partecipazione del personale sanitario.

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

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

Il trattamento dei dati personali nello studio CARE (NIS102061) è conforme al principio di minimizzazione dei dati previsto dall'art. 5, par. 1, lett. c) del GDPR.
Lo studio prevede la raccolta esclusivamente dei dati clinici, demografici e biologici strettamente necessari per il raggiungimento degli obiettivi scientifici dichiarati nel protocollo, ossia l'analisi retrospettiva dei percorsi terapeutici e degli esiti nei pazienti con carcinoma mammario triplo negativo (TNBC).
In particolare:

- Il sistema elettronico eCRF è programmato per vincolare la raccolta ai soli campi obbligatori, corrispondenti a variabili scientificamente rilevanti.
- Non vengono raccolti dati identificativi diretti (es. nome, codice fiscale, indirizzo).
- I dati genetici (es. BRCA1/2) vengono trattati solo se presenti in cartella clinica, senza eseguire test addizionali.
- Nessuna informazione sovrabbondante o ridondante è prevista dal protocollo.
- L'inserimento dei dati è effettuato esclusivamente da personale autorizzato e formato, secondo procedure standardizzate condivise con la CRO e lo sponsor.
- È vietato registrare nelle note dell'eCRF qualsiasi informazione che consenta l'identificazione diretta dei pazienti.

Infine, l'elenco dei pazienti associati ai codici pseudonimi è conservato esclusivamente presso il centro sperimentale, separato e protetto, e non è mai condiviso con sponsor o terze parti.

4.1.4 I dati sono esatti e aggiornati?

I dati trattati nell'ambito dello studio osservazionale CARE (NIS102061) sono esatti, coerenti e aggiornati rispetto alla finalità di ricerca retrospettiva per cui vengono raccolti, in conformità con il principio di esattezza di cui all'art. 5, par. 1, lett. d) del GDPR.
Nello specifico:

- I dati provengono direttamente dalle cartelle cliniche ufficiali archiviate presso l'Istituto Nazionale dei Tumori IRCCS "Fondazione G. Pascale", che rappresentano la fonte primaria e certificata di informazioni cliniche.
- L'inserimento dei dati viene effettuato manualmente da personale sanitario autorizzato, debitamente formato e istruito sulla coerenza e completezza dei dati.
- Il sistema eCRF è dotato di controlli automatici di coerenza (validation rules) per ridurre il rischio di errori o incongruenze.
- Sono previste attività di monitoraggio e revisione da parte della CRO incaricata per garantire l'accuratezza delle informazioni.
- In caso di aggiornamenti clinici rilevanti intercorsi prima della chiusura della raccolta dati, è prevista la modifica dei dati già inseriti a cura dell'investigatore, nel rispetto delle SOP (Standard Operating Procedures).

Poiché si tratta di dati storici (periodo osservazionale 2018–2021), l'aggiornamento si riferisce esclusivamente alla verifica della correttezza rispetto alle fonti originarie. Nessuna manipolazione o integrazione esterna è prevista.

4.1.5 Qual è il periodo di conservazione dei dati?

Il ciclo di conservazione dei dati pseudonimizzati dello studio osservazionale CARE (NIS102061) prevede le seguenti fasi, in linea con le norme nazionali e internazionali:

1. Conservazione presso il centro sperimentale
    - I dati originali e i codici di pseudonimizzazione sono conservati localmente presso l'Istituto "Fondazione G. Pascale" per il tempo necessario alla condivisione e archiviazione interna, in linea con le policy sanitarie vigenti.
2. Conservazione presso sponsor e CRO
    - I dati pseudonimizzati, trasferiti alla CRO e successivamente allo sponsor (MSD), saranno conservati per un periodo di 5 anni dalla chiusura dello studio, rispettando le Good Pharmacoepidemiology Practices (GPP).
3. Eliminazione dei dati
    - Trascorso il periodo di retention:
        - I dati pseudonimizzati saranno cancellati in modo sicuro sia nei sistemi dello sponsor/CRO sia nei sistemi interni del centro, secondo le Policy aziendali e le procedure GPP.
        - Le copie di backup saranno anch'esse eliminate.
4. Audit trail e registrazioni
    - Anche dopo la cancellazione, i metadati e i registri (audit logs) relativi agli accessi e modiche restano conservati, se necessario a fini di compliance, per i tempi richiesti dalla normativa interna sui sistemi, purché questi non contengano dati personali.

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

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

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

Pazienti viventi e contattabili

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

Pazienti deceduti o non rintracciabili

- Ai sensi dell'art. 14 GDPR e dell'art. 110 del Codice Privacy, viene pubblicata un'informativa specifica, redatta dallo sponsor e approvata dal Comitato Etico.
- Le modalità previste includono:
  - Pubblicazione sul sito web dello sponsor (MSD Italia).
  - Pubblicazione sul sito web del centro sperimentale (Istituto Pascale).
  - Affissione di pannelli informativi presso la struttura.
- Se un paziente si ripresenta in reparto (es. per follow-up), il ricercatore ha l'obbligo di:
  - Informarlo tempestivamente,
  - Acquisire il consenso esplicito per il proseguimento del trattamento.

Operatori sanitari (HCP) coinvolti nello studio

- Ricevono un'apposita informativa privacy per personale di ricerca, contenente finalità (es. gestione contrattuale e organizzativa dello studio), tempi di conservazione e modalità di trattamento.
- Non è richiesto il consenso, in quanto il trattamento si basa su obblighi contrattuali e di interesse legittimo (art. 6(1)(b) e (f) GDPR).

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

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

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

Modalità di acquisizione del consenso

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

Revoca del consenso

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

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

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

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

Diritto di Accesso

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

Procedura per Esercitare il Diritto di Accesso

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

Diritto di Portabilità dei Dati

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

Procedura per Esercitare il Diritto di Portabilità dei Dati

1. **Richiesta di Portabilità**:
    - I pazienti possono presentare una richiesta per ottenere i loro dati personali in un formato portabile. La richiesta può essere effettuata al DPO.

- Informazioni di contatto per le richieste di accesso sono generalmente fornite nel documento di informativa al trattamento dei dati e includono l'indirizzo e-mail del DPO.

2. **Verifica dell'Identità**:
   - Come per il diritto di accesso, l'Istituto verificherà l'identità del richiedente per garantire che i dati personali siano rilasciati alla persona corretta.
3. **Fornitura dei Dati**:
   - I dati personali saranno forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico (ad esempio, formato CSV o XML).
   - Se richiesto, i dati possono essere trasmessi direttamente a un altro titolare del trattamento indicato dal paziente, a condizione che ciò sia tecnicamente fattibile.

Contatti per Esercitare i Diritti

- **DPO**: Ing. Alessandro Manzoni
  - **E-mail**: a.manzoni@istitutotumori.na.it
- **Principal Investigator**: Dott. Michelino De Laurentiis
  - **E-mail**: m.delaurentiis@istitutotumori.na.it
  - **Telefono**: +393387858281

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:

1. 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 (es. codice eCRF, se disponibile).
   - Il centro, in quanto titolare autonomo del trattamento, è responsabile della gestione iniziale della richiesta.
2. Allo Sponsor (MSD Italia S.r.l.)
   - L'interessato può scrivere direttamente all'indirizzo email: privacy.italy@msd.com indicando il proprio codice identificativo e il centro presso cui è stato arruolato.
   - MSD, in qualità di titolare del trattamento dei dati pseudonimizzati, prenderà in carico la richiesta, anche se non è in grado di identificare direttamente il paziente senza collaborazione del centro.

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

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

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

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

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

1. 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 la CRO o con lo sponsor.

2. Contatto diretto con lo sponsor (MSD Italia S.r.l.)
   - L'interessato può scrivere a: privacy.italy@msd.com indicando il proprio codice dello studio (se disponibile) e il centro di arruolamento.
   - MSD, in qualità di titolare del trattamento dei dati pseudonimizzati, può applicare la limitazione (es. congelamento dell'uso dei dati) o valutare l'opposizione.

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?

Nell'ambito dello studio osservazionale non interventistico CARE (protocollo NIS102061), promosso da MSD Italia S.r.l., gli obblighi dei responsabili del trattamento sono stati formalmente definiti e regolati da contratti scritti conformi all'articolo 28 del GDPR.

Responsabile del trattamento
Lo sponsor ha nominato la CRO quale responsabile del trattamento ai sensi dell'art. 28 GDPR, mediante un contratto che specifica in dettaglio:

- Le istruzioni documentate impartite da MSD per il trattamento dei dati;
- Le finalità specifiche (es. raccolta dati eCRF, monitoraggio, gestione informatica);
- Le misure tecniche e organizzative di sicurezza da adottare (inclusa pseudonimizzazione, autenticazione, audit);
- Il divieto di trattare i dati per finalità proprie;
- Le modalità di designazione e controllo dei sub-responsabili, ove previsti (es. fornitori IT);
- Le disposizioni in materia di riservatezza del personale autorizzato;
- La possibilità per lo sponsor di effettuare audit e ispezioni;
- Le modalità di restituzione o cancellazione dei dati al termine del contratto.

Centro sperimentale – Istituto Nazionale dei Tumori IRCCS "Fondazione G. Pascale"
L'Istituto agisce come titolare autonomo del trattamento, in relazione alla raccolta e pseudonimizzazione dei dati. Tuttavia, interagisce con i responsabili incaricati dal promotore sulla base di:

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

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

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

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

5. Motivi della valutazione d'impatto

La DPIA è stata realizzata per valutare i potenziali rischi che possono derivare dall'attività di raccolta, gestione ed analisi dei dati nei confronti degli interessati, onde poter garantire un intervento preventivo attraverso opportune misure di sicurezza.
L'esecuzione della DPIA è stata ritenuta necessaria in ragione:

- lo studio prevede il trattamento di dati sensibili, tra cui informazioni cliniche relative a diagnosi e trattamenti del carcinoma TNBC.
- lo studio prevede il trattamento di dati di soggetti vulnerabili: pazienti con carcinoma TNBC

La DPIA è stata ritenuta necessaria in ragione delle linee guida e dei requisiti specificati nel Provvedimento del Garante n. 146/2019. La valutazione d'impatto assicura che tutti i rischi associati al trattamento dei dati personali siano identificati e mitigati adeguatamente, garantendo la protezione dei diritti e delle libertà degli interessati e assicurando la conformità con le normative sulla protezione dei dati.

6. Valutazione dei Rischi

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

6.1 Accesso illegittimo ai dati

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

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

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

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

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

6.1.3 Quali sono le fonti di rischio?

Umano, Strumenti vulnerabili.

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

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

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

Importante/Grave

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

Poco Probabile

6.2 Modifiche indesiderate dei dati

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

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

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

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

Inoltro di dati a soggetti non autorizzati a conoscerli.
Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto).

6.2.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano

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

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

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

Importante/Grave

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

Poco probabile

6.3 Perdita di dati

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

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

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

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

6.3.3 Quali sono le fonti di rischio?

Strumenti vulnerabili, Umano.

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

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

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

Grave/Importante

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

Poco Probabile

7. Piano d'azione

7.1 Mitigazione dei rischi con Misure esistenti o pianificate

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

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

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

7.1.4 Politica di tutela della privacy

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

7.1.5 Gestione delle politiche di tutela della privacy

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

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

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

7.1.6 Minimizzazione dei dati

L'eCRF 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 eCRF consente l'accesso solo a utenti autorizzati con autenticazione mediante credenziali individuali (user/password).
Tutte le operazioni sono tracciate tramite log di accesso e controlli periodici di sicurezza.

7.1.8 Limitazione dell'Accesso ai Dati

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

7.1.9 Audit e monitoraggi periodici

Saranno condotti audit periodici e controlli interni per verificare la conformità alle politiche di sicurezza e alle normative sulla protezione dei dati.
Il contratto tra sponsor e responsabili prevede diritto di audit e ispezioni, anche on-site, per verificare la conformità al GDPR e alle misure di protezione concordate.

7.1.10 Sicurezza dei canali informatici

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

7.1.11 Procedure di sicurezza dei sistemi elettronici

I server che ospitano i dati sono collocati in ambienti protetti, con accesso fisico limitato al personale autorizzato.
I sistemi elettronici includono soluzioni di ridondanza per prevenire la perdita dei dati in caso di guasti.
I server sono protetti da firewall configurati per bloccare accessi non autorizzati.

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

7.1.12 Accesso controllato ai locali
Accesso al reparto con badge.

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

7.2 Panoramica dei rischi

7.2.1 Analisi complessiva del dell'entità del rischio

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

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

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

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

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

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

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

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

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
Accesso illegittimo ai dati	Violazione della Privacy, Implicazioni Psicologiche e Sociali, Discriminazione, Costi, Diffusione risultati della ricerca	Vulnerabilità informatiche, attacco basato su chiave compromessa, attacco denial of service di rete, spoofing d'identità, attacco man in the middle, attacco di riproduzione RTP, virus, worm, phishing, malware. Locale lasciato aperto o non custodito. Trasmissione informatica o comunicazione verbale di dati personali a soggetti non autorizzati. Accesso e/o trattamento dei dati personali per finalità diverse da quelle autorizzate. Allontanarsi dalla propria postazione lasciando il PC connesso. Copiare i dati su dispositivi removibili e trasportabili all'esterno senza autorizzazione. 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, Contrattualizzazione con Responsabili Esterni.	Grave	Poco probabile	**Medio**	Limitata/Improbabile	**Basso**

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		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, Contrattualizzazione con Responsabili Esterni.	Grave	Poco probabile	**Medio**	Limitata/Improbabile	**Basso**

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		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.	Grave	Poco probabile	**Medio**	Limitata/Improbabile	**Basso**

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		phishing, malware. Locale lasciato aperto o non custodito. Allontanarsi dalla propria postazione lasciando il PC connesso.						

La verifica dell'implementazione delle MIT identificate sarà effettuata a 12 mesi dalla data di emissione del documento e comunque prima dell'eventuale chiusura dello studio. Conseguentemente sarà aggiornata la tabella di analisi dei rischi ed il documento corrente.

8. Risultato della DPIA

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

Risultati della valutazione d'impatto	
☐ **Rischio residuo elevato**	☒ **Rischio residuo non elevato**
Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento non sono ritenute sufficienti. Il rischio residuale per i diritti e le libertà degli interessanti resta elevato.	Le misure tecniche e organizzative individuate per mitigare l'impatto del trattamento sono ritenute sufficienti.

Il Titolare del trattamento – a seguito dei risultati della DPIA - pertanto dichiara che le misure riducono significativamente la probabilità e l'impatto dei rischi.

A seguito dell'analisi dettagliata e sistematica dei trattamenti dei dati personali nel progetto "CARE", 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.