	Nome e Cognome	Ruolo	Firma	Data
Redazione	Roberta Fusco	Ingegnere Biomedico		28/01/25
	Elisa Pintauro	Ricercatore sanitario		20/1/25
Revisione	Gianfranco De Feo	Quality Assurance		30/01/2025
	Maurizio Di Mauro	Titolare del trattamento dati		30.01.2025
	Alessandro Manzoni	DPO		28/01/2025
Approvazione	Roberta Caputo	Sperimentatore Principale Centro Satellite		21/01/2025
	Gianfranco De Feo	Quality Assurance		23/01/2025

Tracking delle modifiche

N° Rev.	Data	Motivo della modifica	Paragrafi	Pagine
0	20.01.2025	Prima emissione	TUTTI	TUTTE

Storico della rivalutazione

Revisione annuale della DPIA o a seguito di verifiche/minacce

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

	Data prevista	Data effettiva	Firma
Rivalutazione a cura del QA			

Titolo dello studio	Sviluppo di un test composito per la gestione del cancro alla mammella HER2-positivo in stadio precoce – Studio HERCard – nell'ambito del progetto PNRR-POC-2023-12378113 "A composite assay for Her2-positive early-stage breast cancer management"
Promotore	Istituto Nazionale Tumori - IRCCS - Fondazione Pascale
Centro coordinatore	Istituzione: Fondazione IRCCS Istituto Nazionale dei Tumori di Milano
Centro Satellite	Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Collaboratore Principale Centro Satellite	Dr.ssa Roberta Caputo S.C. Oncologia Clinica Sperimentale di Senologia Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale
Tipologia di studio	Studio osservazionale biologico retrospettivo multicentrico
Parere del Comitato Etico	Determina Dirigenziale N. 1059 del 05/08/202 Parere favorevole del Comitato Etico Territoriale competente (CET Campania 1), rilasciato nella seduta del 10.07.2024
Durata dello studio	6-8 mesi
DPO/RPD	Ing. Alessandro Manzoni

Tabella dei Contenuti

1. Nozione di valutazione d'impatto

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.

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 Istituto Nazionale Tumori di Napoli, IRCCS G. Pascale è il Legale Rappresentante e la dr.ssa Roberta Caputo, quale delegato in qualità di sperimentatore principale presso il Centro.

3.2 Soggetti interessati

L'attività interessa il trattamento di dati riguardanti:

- pazienti già in precedenza assistiti presso

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

- pazienti che hanno fornito in precedenza propri campioni biologici presso

ISTITUTO DI RICOVERO E CURA A CARATTERE SCIENTIFICO "Fondazione Giovanni Pascale" – NAPOLI
Lo studio sarà condotto su dati clinico-patologici già raccolti (analisi retrospettiva) e sulla loro integrazione con dati di espressione genica di campioni tumorali ottenuti da procedure diagnostiche e terapeutiche di routine, ovvero di tessuto eccedente quello necessario per la diagnosi, prelevato alla biopsia o all'intervento chirurgico e conservati in formalina e paraffina (FFPE).

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

- Altro

NA

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 campioni biologici e i relativi dati clinici sono stati pseudonimizzati. Non vi è alcun utilizzo di dati biometrici, sensibili o correlati a individui identificabili.
- Lo studio attuale non comporta la raccolta di nuovi dati o campioni direttamente dai pazienti. L'analisi si basa esclusivamente su campioni e dati già esistenti, riducendo significativamente il rischio per la privacy o la sicurezza degli interessati.
- 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.

N.B. La presente DPIA è stata redatta anche considerando la Valutazione di Impatto fatta dal Promotore dello Studio INT di Milano

3.3 Descrizione del trattamento

3.3.1 Quale è il trattamento in considerazione?

Il trattamento in considerazione, descritto nel protocollo HERCard, riguarda pazienti affetti da carcinoma mammario HER2-positivo in stadio precoce. In particolare, si analizzano pazienti trattati con terapia **neoadiuvante e/o adiuvante** basata sull'uso di **trastuzumab,** spesso associato a **pertuzumab** e chemioterapia. L'obiettivo principale è sviluppare un test prognostico composito basato su un classificatore genomico (S18) integrato con variabili clinico-patologiche per migliorare la gestione terapeutica e prevedere la sopravvivenza.
Lo studio sarà condotto su dati clinico-patologici già raccolti (analisi retrospettiva) e sulla loro integrazione con dati di espressione genica di campioni tumorali ottenuti da procedure diagnostiche e terapeutiche di
routine, ovvero di tessuto eccedente quello necessario per la diagnosi, prelevato alla biopsia o all'intervento chirurgico e conservati in formalina e paraffina (FFPE).

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 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. Responsabile del Trattamento dei Dati (Data Processor)

Il Responsabile del Trattamento dei Dati è una terza parte che tratta i dati personali per conto del Titolare del Trattamento.

Per codesto progetto, questo ruolo è stato delegato al Collaboratore Principale del Centro Satellite nella persona della Dr.ssa Roberta Caputo.

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 campioni e i dati clinici secondo le linee guida stabilite nel protocollo dello studio.
Gestire i dati clinici e genomici: I dati raccolti e analizzati sono conservati in database elettronici protetti e accessibili solo al personale autorizzato.
Garantire la riservatezza: Trattare i dati in modo anonimo e rispettare il principio di minimizzazione, limitando il trattamento ai dati strettamente necessari per gli scopi dello studio.
Rispettare i diritti degli interessati: Garantire che gli interessati possano esercitare i loro diritti, come l'accesso ai dati, la rettifica e il ritiro del consenso.

3.3.3 Ci sono standard applicabili al trattamento?

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

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

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

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

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

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

3.4 Dati, processi e risorse di supporto

3.4.1 Quali sono i dati trattati?

I dati trattati nel contesto del protocollo HERCard includono informazioni clinico-patologiche e genomiche dei pazienti con carcinoma mammario HER2-positivo. In dettaglio, si raccolgono e analizzano i seguenti tipi di dati:
1. Dati personali:
   - Sesso
   - Data di nascita
   - Altezza e peso
2. Informazioni sulla diagnosi:
   - Data della biopsia
   - Tipo istologico del tumore
   - Stato dei recettori ormonali (ER e PgR)

- Valori di Ki-67
- Presenza di linfociti infiltranti il tumore (TIL)
- Istotipo e grado tumorale
- Stato HER2 (immunoistochimica e amplificazione del gene ERBB2)

3. Informazioni sul trattamento:
   - Tipo di trattamento neoadiuvante e/o adiuvante (es. trastuzumab ± pertuzumab)
   - Terapie ricevute e relative risposte (inclusa la risposta patologica completa - pCR)
4. Dati sul follow-up:
   - Esiti clinici (es. sopravvivenza libera da eventi - EFS, sopravvivenza globale - OS)
   - Eventuali recidive e malattia residua
5. Dati genomici:
   - Profili di espressione genica relativi a 18 geni del classificatore S18
   - Cambiamenti nell'espressione genica pre e post-trattamento
   - Analisi dei file **Nanostring** e **RT-PCR** delle biopsie.
6. Dati strutturati per la ricerca:
   - Ogni paziente viene identificato da un codice pseudoanonimo (record_id) per proteggere la riservatezza. Non sono registrati nome e cognome, evitando la reidentificazione diretta

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

Il ciclo di vita del trattamento dei dati nel contesto dello studio HERCard segue un processo strutturato che garantisce la raccolta, la gestione e l'analisi dei dati in modo sicuro e conforme alle normative. Ecco una descrizione funzionale delle fasi principali del ciclo di vita:

1. Raccolta dei dati
   - Origine dei dati: I dati vengono raccolti da cartelle cliniche e campioni biologici relativi a pazienti con carcinoma mammario HER2-positivo.
   - Tipologie di dati raccolti:
     - Dati clinici (es. diagnosi, trattamenti ricevuti, esiti clinici).
     - Dati biologici/genomici (profili di espressione genica mediante Nanostring e RT-PCR).
     - Dati personali pseudonimizzati (es. sesso, data di nascita, altezza, peso).
   - Modalità di raccolta:
     - I dati clinici vengono estratti dalle cartelle cliniche da personale addestrato.
     - I campioni biologici (es. tessuti tumorali) vengono processati per analisi genomiche.
2. Pseudonimizzazione dei dati

   Ogni paziente viene identificato tramite un codice univoco (record_id) generato dalla piattaforma REDCap. Questo codice sostituisce i dati identificativi personali (nome, cognome), garantendo l'anonimato e limitando il rischio di reidentificazione.

   La mappatura tra codice e dati personali è accessibile solo ai ricercatori autorizzati.
3. Conservazione dei dati
   - Supporti e piattaforme:
     - Dati clinici e genomici vengono memorizzati in REDCap, una piattaforma sicura che garantisce autenticazione e tracciabilità degli accessi.

- I campioni biologici sono conservati in paraffina (FFPE) presso i centri partecipanti (es. Istituto Pascale e Ospedale Di Summa-Perrino).
- Durata della conservazione: I dati vengono conservati per un periodo minimo di 25 anni, come previsto dai requisiti di ricerca e normativi.

4. Analisi dei dati
   - Scopo delle analisi:
     - Validare il valore prognostico del classificatore genomico S18.
     - Integrare i dati genomici con variabili clinico-patologiche per sviluppare un test prognostico composito.
   - Tipologie di analisi:
     - Analisi statistica (es. modelli di regressione di Cox, log-rank test).
     - Analisi genomica (es. profili di espressione genica tramite Nanostring e RT-PCR).
   - Strumenti utilizzati:
     - Software specifici per analisi statistica (es. R, nSolver).
5. Condivisione e reportistica
   I risultati delle analisi vengono condivisi con i ricercatori autorizzati e utilizzati per sviluppare strategie di trattamento personalizzate.
   I dati anonimi possono essere condivisi con partner di ricerca o terze parti per finalità scientifiche, previa conformità con il GDPR.
6. Archiviazione a lungo termine
   I dati codificati vengono archiviati in modo sicuro per futuri utilizzi di ricerca, a condizione che il consenso informato lo consenta.
   Eventuali trasferimenti di dati all'estero sono soggetti a specifiche salvaguardie (es. contratti o clausole di protezione dati).
7. Eliminazione dei dati
   I dati non possono essere eliminati durante il periodo minimo di conservazione (25 anni) per garantire la validità della ricerca e soddisfare i requisiti legali.
   Dopo tale periodo, i dati possono essere distrutti o conservati ulteriormente per scopi di ricerca, seguendo le normative vigenti.

3.4.3 Quali sono le risorse di supporto ai dati?

Le risorse di supporto ai dati per lo studio HERCard includono strumenti, infrastrutture, piattaforme e personale specializzato utilizzati per la gestione, l'analisi e la sicurezza dei dati clinici e genomici.

1. Piattaforme di gestione dei dati
   - REDCap (Research Electronic Data Capture)
   - Una piattaforma sicura utilizzata per creare e gestire i moduli elettronici per la raccolta dei dati (eCRF, electronic Case Report Forms).

   Caratteristiche principali:
   Accesso controllato: Solo il personale autorizzato dal Principal Investigator può accedere.
   Tracciabilità: Ogni attività è registrata per prevenire usi impropri.
   Pseudonimizzazione: I pazienti sono identificati tramite un codice (record_id), che elimina informazioni sensibili come nome e cognome.
   Caricamento dati: Dati personali, clinico-patologici, diagnostici e file genomici (Nanostring e RT-PCR).

2. Campioni biologici
   I campioni tumorali sono conservati in paraffina (FFPE) presso i centri partecipanti.
   Questi campioni vengono utilizzati per analisi genomiche e molecolari (es. profili di espressione genica) e sono fondamentali per lo studio.
3. Infrastrutture di analisi genomica
   Tecnologie di profiling:
   Nanostring: Per l'analisi di espressione genica con precisione.
   RT-PCR (Reverse Transcription Polymerase Chain Reaction): Per la quantificazione dell'RNA tumorale.
   Software per analisi genomiche:
   nSolver: Specifico per la piattaforma Nanostring, consente la normalizzazione e l'analisi statistica dei dati di espressione genica.
   Pacchetti R: Per ulteriori analisi bioinformatiche e statistiche.
4. Personale specializzato
   Ricercatori e analisti bioinformatici:
   Si occupano della progettazione e implementazione delle analisi statistiche e bioinformatiche.
   Personale addestrato alla raccolta dati:
   Responsabili della raccolta e dell'archiviazione di informazioni cliniche presso i centri partecipanti.
   Coordinamento centrale:
   La Fondazione IRCCS Istituto Nazionale dei Tumori di Milano coordina l'analisi bioinformatica e statistica dei dati anonimizzati, ma non partecipa alla raccolta diretta di campioni o dati clinici.
5. Sicurezza
   Misure di sicurezza:
   Controllo degli accessi: Basato su autenticazione e autorizzazione specifica.
   Crittografia: Per proteggere i dati durante il trasferimento e l'archiviazione.
   Backup Regolari:
   - Implementazione di backup periodici dei dati per prevenire la perdita di informazioni. Il database elettronico è allocato sulla rete intranet e pertanto segue le regole aziendali di backup.
6. Infrastruttura IT
   Server sicuri per la memorizzazione e il backup dei dati.
   Strumenti di monitoraggio per garantire la qualità e l'integrità dei dati.
7. Infrastruttura Fisica
   - Laboratori:
     - I laboratori presso l'Istituto Nazionale Tumori – Fondazione Pascale e altri centri coinvolti sono attrezzati per:
       - La conservazione dei campioni biologici.
       - L'esecuzione di analisi genetiche avanzate (sequenziamento).
   - Strutture di conservazione dei campioni:
     - Freezer a temperatura controllata (-80°C o inferiore) per la conservazione a lungo termine dei campioni biologici.
     - Sistemi di catalogazione e tracciabilità dei campioni.
8. Normative e Linee Guida
   - Conformità Regolamentare:

- Adesione a normative come il GDPR, la Dichiarazione di Helsinki e le Linee Guida per la Buona Pratica Clinica (CPM/ICH135/95-DM 15/7/97).
- Procedure Standardizzate:
  - Implementazione di procedure standardizzate per la raccolta, gestione e analisi dei dati.

9. Supporto Privacy
   - Supporto privacy:
     - Consulenza per assicurare la conformità alle normative sulla protezione dei dati personali.
   - Supporto scientifico/assicurazione di Qualità:
     - Gestione amministrativa per la documentazione, consenso informato e comunicazioni con enti regolatori.
     - Revisione della documentazione da parte della Commissione Interna Studi Clinici
     - Monitoraggio/audit periodici
     - Presenza di specifiche Procedure
10. Risorse finanziarie
    - Finanziamento del progetto:
      - Fondi stanziati dal Ministero della Salute nell'ambito del PNRR (Piano Nazionale di Ripresa e Resilienza).
      - Budget dedicato all'acquisto di attrezzature, materiali di laboratorio e supporto tecnico.

Queste risorse combinano tecnologia, infrastruttura, personale e procedure per supportare efficacemente la gestione dei dati nello studio, assicurando la qualità, la sicurezza e la conformità dei dati trattati.

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. Principi Fondamentali

4.1 Proporzionalità e necessità

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

I dati personali sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo compatibile con tali finalità. I dati raccolti nello studio "HERCard" vengono utilizzati esclusivamente per gli scopi dichiarati nel protocollo di ricerca.

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

I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti degli interessati. I partecipanti allo studio "HERCard" ricevono un'informativa dettagliata e comprensibile che spiega lo scopo della ricerca, le modalità di trattamento dei dati, e i diritti degli interessati. Viene ottenuto un consenso informato allo studio.

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

I dati raccolti sono limitati a quanto strettamente necessario per raggiungere gli obiettivi dello studio:

- **Pseudonimizzazione**: Non vengono raccolti dati identificativi diretti (es. nome, cognome). Ogni paziente è identificato tramite un codice univoco (record_id) generato dalla piattaforma REDCap.
- **Campioni biologici**: Solo i campioni in eccedenza dalla routine clinica vengono utilizzati per l'analisi. Nessun campione viene prelevato esclusivamente a fini di ricerca.
- **Dati clinici**: Sono raccolte solo le informazioni rilevanti per analizzare la risposta terapeutica e le variabili prognostiche (es. stato HER2, Ki-67, recettori ormonali, TILs).
- **Dati genomici**: L'analisi si concentra su un set specifico di geni (18 geni del classificatore S18), riducendo il rischio di raccolta eccessiva o superflua.

4.1.4 I dati sono esatti e aggiornati?

I dati personali sono trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione contro trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentali. Vengono utilizzate misure di sicurezza tecniche avanzate per proteggere i dati dei partecipanti che, inoltre, sono trattati da personale soggetto agli obblighi previsti in materia di segreto d'ufficio, segreto professionale e deonologico.

4.1.5 Qual è il periodo di conservazione dei dati?

I dati personali sono conservati in una forma che consente l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati raccolti nell'ambito dello studio "HERCard" sono conservati per 25 anni; in ogni caso, i dati saranno conservati esclusivamente per la durata strettamente necessaria al completamento del progetto di ricerca e adempimenti in relazione alla materia brevettuale. L'applicativo consente la cancellazione dei dati su richiesta del principal investigator dello studio.

4.2 Misure a tutela dei diritti degli interessati

4.2.1 Come sono informati del trattamento gli interessati?

Gli interessati dello studio HERCard (pazienti con carcinoma mammario HER2-positivo) vengono informati del trattamento dei loro dati attraverso un processo strutturato, che garantisce trasparenza, chiarezza e conformità alle normative etiche e legali. Di seguito i principali strumenti e metodi utilizzati:

1. Foglio informativo per il paziente
   - Un foglio informativo dettagliato viene fornito ai pazienti per spiegare il trattamento dei dati. Questo documento include:
   - Descrizione dello studio:
     - Obiettivi dello studio HERCard.
     - Modalità di raccolta e trattamento dei dati.
     - Benefici attesi e potenziali rischi.
   - Tipologia di dati trattati:
     - Dati clinici, patologici, genomici e personali pseudonimizzati.
   - Modalità di conservazione e sicurezza:
     - Pseudonimizzazione dei dati per proteggere l'identità.
     - Archiviazione sicura in piattaforme come REDCap.

2. Consenso informato scritto

Prima di partecipare, ogni paziente deve firmare un modulo di consenso informato.
   - Il consenso viene raccolto per autorizzare:
     - Il trattamento dei dati personali e clinici.
     - L'uso di campioni biologici per analisi genomiche.
   - Firma e data:
     - Una copia del modulo firmato è consegnata al paziente, mentre l'originale è archiviato nel registro clinico dello studio.
   - Trasparenza:
     - Il ricercatore responsabile spiega verbalmente la natura, gli obiettivi e i potenziali rischi dello studio per garantire una scelta informata.

3. Informazioni sui diritti degli interessati

I pazienti vengono informati che hanno diritto a:
   - Revocare il consenso in qualsiasi momento, senza conseguenze sulla qualità del trattamento medico ricevuto.

4. Informativa sulla riservatezza
   - I pazienti sono informati che i dati raccolti saranno pseudonimizzati (cioè associati a un codice univoco) e non includeranno informazioni identificative dirette come nome e cognome.
   - Solo il personale autorizzato può accedere ai dati originali, necessari per la conduzione dello studio clinico.
   - Eventuali trasferimenti di dati a terzi (per collaborazioni di ricerca) avverranno in forma codificata e anonima, nel rispetto del GDPR e delle normative nazionali.

5. Aggiornamenti e modifiche
   - Eventuali aggiornamenti sono comunicati attraverso i canali ufficiali dello studio.

6. Trattamento dei dati di pazienti deceduti o non reperibili
   - Nel caso di pazienti deceduti o non reperibili, lo studio si avvale dell'esenzione dal consenso per continuare a utilizzare i dati anonimi, come previsto dalle normative sulla ricerca retrospettiva.

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

Prima di partecipare, ogni paziente deve firmare un modulo di consenso informato.
Il consenso viene raccolto per autorizzare:
Il trattamento dei dati personali e clinici.
L'uso di campioni biologici per analisi genomiche.
Firma e data:
Una copia del modulo firmato è consegnata al paziente, mentre l'originale è archiviato nel registro clinico dello studio.
Trasparenza:
Il ricercatore responsabile spiega verbalmente la natura, gli obiettivi e i potenziali rischi dello studio per garantire una scelta informata.

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

In qualunque momento, i partecipanti hanno il diritto di ottenere conferma del trattamento dei loro dati personali e di accedere a tali dati, ai sensi dell'articolo 15 del Regolamento (UE) 2016/679 (GDPR). Gli interessati possono esercitare il loro diritto di accesso richiedendo e ottenendo una copia dei propri dati personali raccolti durante lo studio, conformemente a quanto previsto dall'articolo 15 del GDPR. L'esercizio dei diritti da parte degli interessati sarà consentito conformemente a quanto descritto nella procedura aziendale e pubblicato nella sezione privacy del sito istituzionale.

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

In qualunque momento, i partecipanti hanno il diritto di richiedere la rettifica dei propri dati personali inesatti, ai sensi dell'articolo 16 del Regolamento (UE) 2016/679 (GDPR). Gli interessati possono segnalare eventuali inesattezze nei loro dati personali e ottenere la tempestiva rettifica di tali errori, in conformità con quanto previsto dall'articolo 16 del Regolamento (UE) 2016/679 (GDPR).
L'esercizio dei diritti da parte degli interessati sarà consentito conformemente a quanto descritto nella procedura aziendale e pubblicato nella sezione privacy del sito istituzionale.
Il diritto di cancellazione, stabilito dall'articolo 17 del GDPR, consente
all'interessato di richiedere la cancellazione dei propri dati quando, per esempio, non sono più necessari. Tuttavia, in ambito di ricerca scientifica, l'articolo 17, paragrafo 3, lettera d, prevede una deroga per evitare che la cancellazione comprometta gli obiettivi della ricerca. Questo è in linea con l'articolo 89, paragrafo 1, che richiede l'adozione di garanzie adeguate, come la pseudonimizzazione, per proteggere i diritti degli interessati. Il WP29 e l'EDPB, nelle Linee guida 1/2022, specificano che la cancellazione può essere limitata per finalità di ricerca, purché siano adottate misure tecniche e organizzative che garantiscano la protezione dei dati personali.

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

Il diritto di limitazione del trattamento, stabilito dall'articolo 18 del GDPR, consente all'interessato di richiedere una sospensione temporanea del trattamento dei propri dati personali in casi specifici, come ad esempio quando l'interessato contesta l'accuratezza dei dati o ritiene che il trattamento sia illecito. Tuttavia, nel contesto della ricerca scientifica, questo diritto può essere limitato in conformità all'articolo 89, paragrafo 2 del GDPR, qualora la limitazione comprometterebbe seriamente il conseguimento degli obiettivi della ricerca. In particolare, l'articolo 18, paragrafo 2 prevede che, nonostante una richiesta di limitazione, il trattamento può continuare se i dati sono necessari per scopi di ricerca scientifica, purché siano adottate adeguate misure di sicurezza, come la pseudonimizzazione o altre tecniche di protezione.
In qualunque momento, i partecipanti hanno il diritto di opporsi al trattamento dei propri dati personali per motivi connessi alla loro situazione particolare, ai sensi dell'articolo 21 del Regolamento (UE) 2016/679 (GDPR). Ogni richiesta di opposizione viene valutata con attenzione e, in assenza di motivi legittimi prevalenti per proseguire il trattamento, i dati del richiedente cessano di essere trattati, in conformità con quanto previsto dall'articolo 21 del GDPR. L'esercizio dei diritti da parte degli interessati sarà consentito conformemente a quanto descritto nella procedura aziendale e pubblicato nella sezione privacy del sito istituzionale.

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

I rapporti tra titolare e responsabili del trattamento sono regolati da contratti o accordi specifici, in linea con l'Articolo 28 del GDPR. Tali contratti disciplinano:

- Finalità del trattamento:
  - Specificano che i dati possono essere trattati solo per le attività relative allo studio HERCard.
- Misure di sicurezza:
  - Descrivono le misure tecniche e organizzative implementate per proteggere i dati personali.
- Sub-responsabili del trattamento:
  - Regolano l'eventuale coinvolgimento di altri soggetti, come fornitori di servizi IT o laboratori di analisi genomica.
- Audit e ispezioni:
  - Consentono al titolare del trattamento (es. Fondazione IRCCS Istituto Nazionale dei Tumori di Milano) di verificare la conformità del responsabile attraverso audit o altre forme di controllo.
- Durata e conservazione dei dati:
  - Stabiliscono i termini per la conservazione dei dati e la loro eventuale cancellazione al termine dello studio.

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

Il progetto è finalizzato alla presentazione di una domanda brevettuale.
L'eventuale diffusione avverrà esclusivamente dopo l'iter brevettuale tramite pubblicazione di articoli e/o comunicazioni scientifiche di dati aggregati anonimi. Eventuali raw data

anonimi verranno resi disponibili solo su richiesta formale compatibilmente con le regole brevettuali.

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 e dei campioni biologici 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:

- il Trattamento di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni.
- il trattamento non occasionali di dati relativi a soggetti vulnerabili (pazienti).
- il trattamento di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

La DPIA per lo Studio "PNRR-MCNT2-2023-12377133" 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, Gestione delle politiche di tutela della privacy, Minimizzazione dei dati, Limitazione dell'Accesso ai Dati, Accesso controllato ai locali, Logout / disconnessione automatica temporizzata, Audit e monitoraggi periodici, Monitoraggio dello stato degli apparati tecnologici.

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.

6.2.3 Emergenza non sanitaria con impatto sul sistema informatico (incendio, alluvione, terremoto).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, Gestione delle politiche di tutela della privacy, Accesso controllato ai locali, Logout / disconnessione automatica temporizzata, Audit e monitoraggi periodici, Monitoraggio dello stato degli apparati tecnologici.

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 Pseudoanonimizzazione
Ogni paziente viene identificato da un codice pseudoanonimo (record_id) per proteggere la riservatezza. Non sono registrati nome e cognome, evitando la reidentificazione diretta.

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
Uso della piattaforma REDCap

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

- L'accesso è regolato da un sistema di autorizzazioni basato sui ruoli, che limita ciò che ciascun utente può fare (es. inserimento, visualizzazione o analisi dei dati).

- **Registrazione delle attività**:
  - Ogni azione compiuta sulla piattaforma (es. inserimento, modifica o visualizzazione di dati) viene registrata in un **log di audit**.
  - Il log include:
    - Identità dell'utente.
    - Data e ora dell'operazione.
    - Descrizione dell'operazione eseguita.
- **Tracciabilità dei record pseudonimizzati**:
  - I dati dei pazienti sono identificati da un codice pseudonimo (**record_id**), rendendo possibile tracciare l'intero ciclo di vita di ogni record senza esporre dati personali identificativi.

Processi di raccolta e gestione dei dati

- **Tracciabilità dei campioni biologici**:
  - I campioni tumorali sono etichettati con codici anonimi e registrati nei sistemi informativi dei centri partecipanti.
  - Ogni campione è collegato al corrispondente codice pseudonimo (record_id) per mantenere un collegamento controllato tra dati clinici e biologici.

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

Lo studio è finalizzato a sviluppare un **test prognostico composito** per pazienti con carcinoma mammario HER2-positivo, basato su un classificatore genomico (S18) integrato con variabili clinico-patologiche. Per raggiungere questo obiettivo, vengono raccolti **solo i dati strettamente necessari**, sia clinici che genomici.

7.1.7 Controllo degli accessi logici

L'accesso ai dati è limitato al personale autorizzato attraverso:

- Credenziali individuali.
- Criteri di password robusti (es. lunghezza minima, rotazione periodica).

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 altri centri o ricercatori sono resi pseudonimizzati, includendo solo le informazioni strettamente necessarie per le analisi.
L'applicativo utilizzato per creare le eCRF è RedCap che consente l'accesso solo a personale autorizzato dal principal investigator. Ogni utente autorizzato può avere profili di accesso diversi a seconda dell'attività da svolgere sul progetto. L'autenticazione e la tracciabilità limitano l'uso improprio dei dati per scopi non autorizzati. In RedCap non vengono inserite informazioni su nome e cognome del paziente in quanto RedCap in automatico crea un codice pseudoanonimo del paziente (record_id) che non consente all'INT la reidentificazione. In piattaforma REDCap, per ciascun paziente a cui viene attribuito un ID, vengono inseriti dati quali: informazioni personali (sesso, data di nascita, altezza, peso; etc..), informazioni sulla diagnosi (data della biopsia, tipo di istologico; etc..), informazioni sulla chirurgia, sul trattamento e sul follow-up. Infine è richiesto il caricamento dei file Nanostring e PCR delle biopsie analizzate.

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.
Le eCRF sono ospitate su un server presso il Data Center di Arezzo, accessibile tramite protocollo HTTPS per l'applicazione e Windows Remote Access per l'amministrazione. L'architettura hardware e software del server è compliant alle linee guida EMA/FDA.

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.
Backup regolari (giornalieri, settimanali) dei dati sono archiviati in sedi sicure.
I server sono protetti da firewall configurati per bloccare accessi non autorizzati.
Sistemi di rilevamento delle intrusioni (IDS) monitorano continuamente il traffico per individuare comportamenti anomali o potenziali attacchi.
I sistemi sono dotati di software antivirus aggiornati regolarmente per prevenire malware e attacchi informatici.
Tutti i software utilizzati (sistemi operativi, applicazioni) vengono aggiornati periodicamente per risolvere vulnerabilità note.

7.1.12 Accesso controllato ai locali

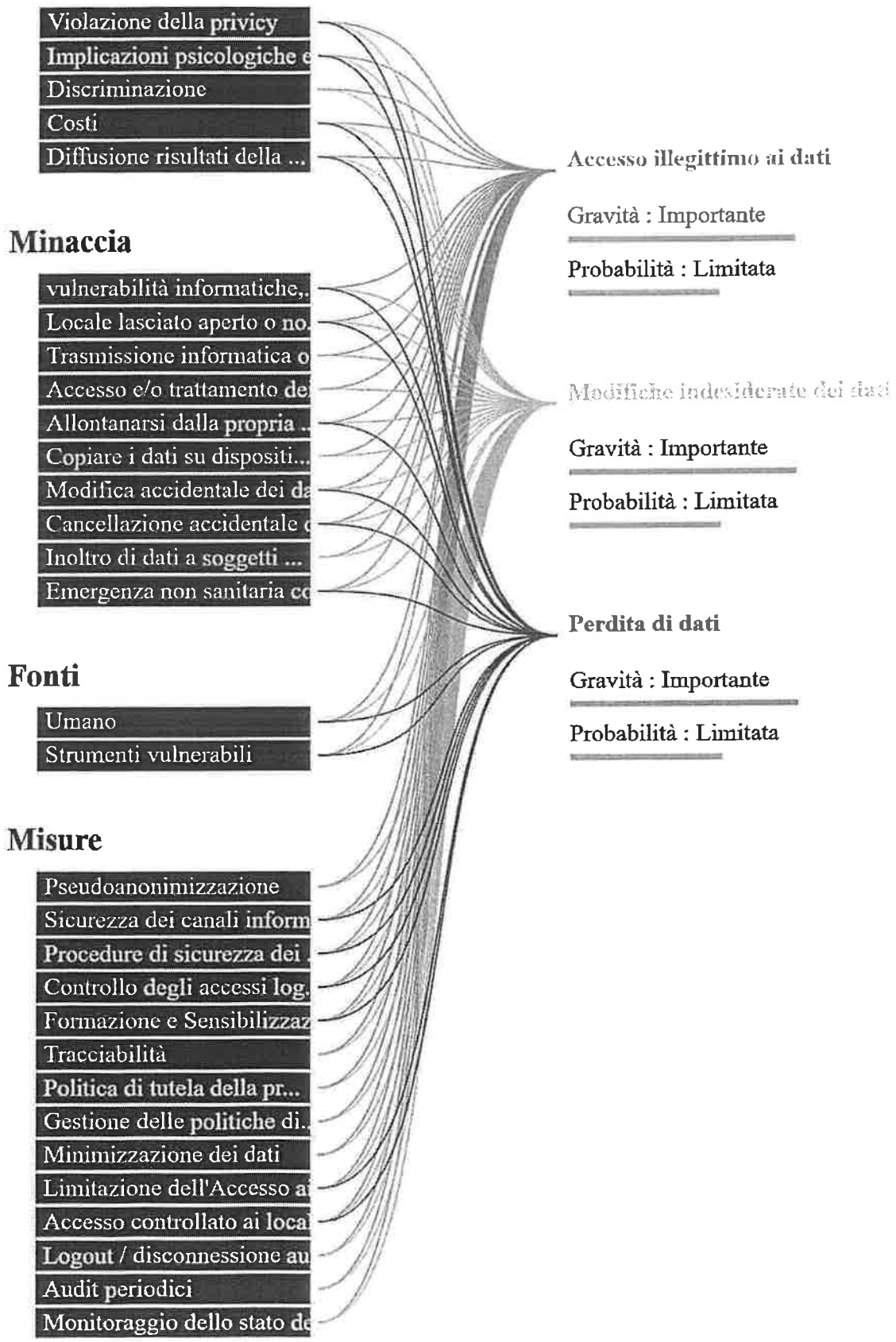
Accesso al reparto con badge.

7.1.13 Logout

Disconnessione automatica temporizzata.

7.1.14 Monitoraggio dello stato degli apparati tecnologici

7.2 Panoramica dei rischi


Impatti potenziali
Violazione della privicy
Implicazioni psicologiche e
Discriminazione
Costi
Diffusione risultati della ...
Minaccia
vulnerabilità informatiche,.
Locale lasciato aperto o no.
Trasmissione informatica o
Accesso e/o trattamento dei
Allontanarsi dalla propria ..
Copiare i dati su dispositi...
Modifica accidentale dei da
Cancellazione accidentale
Inoltro di dati a soggetti ...
Emergenza non sanitaria co
Fonti
Umano
Strumenti vulnerabili
Misure
Pseudoanonimizzazione
Sicurezza dei canali inform
Procedure di sicurezza dei
Controllo degli accessi log.
Formazione e Sensibilizzaz
Tracciabilità
Politica di tutela della pr...
Gestione delle politiche di..
Minimizzazione dei dati
Limitazione dell'Accesso ai
Accesso controllato ai loca
Logout / disconnessione au
Audit periodici
Monitoraggio dello stato de
Accesso illegittimo ai dati
Gravità : Importante
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Importante
Probabilità : Limitata
Perdita di dati
Gravità : Importante
Probabilità : Limitata

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.	Pseudonimizzazione, Formazione e Sensibilizzazione, Tracciabilità, Politica di Tutela della privacy, Gestione delle politiche di tutela della privacy, minimizzazione dei dati, controllo degli accessi logici, Limitazione dell'accesso ai dati, audit e monitoraggi periodici, sicurezza dei canali informatici. Procedure di sicurezza dei sistemi elettronici, accesso controllato ai locali, logout, monitoraggio dello stato degli apparati	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
		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.						
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,	Pseudonimizzazione, Formazione e Sensibilizzazione, Tracciabilità, Politica di Tutela della privacy, Gestione delle politiche di tutela della privacy, minimizzazione dei dati, controllo degli accessi logici, Limitazione	Grave	Poco probabile	**Medio**	Limitata/Improbabile	Basso

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		attacco 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.	dell'accesso ai dati, audit e monitoraggi periodici, sicurezza dei canali informatici. Procedure di sicurezza dei sistemi elettronici, accesso controllato ai locali, logout, monitoraggio dello stato degli apparati					

Rischio	Impatti potenziali	Minacce	Misure di Mitigazione (MIT)	Gravità	Probabilità	ENTITA' COMPLESSIVA DEL RISCHIO	Gravità/Probabilità dopo implementazioni delle MIT	ENTITA' COMPLESSIVA DEL RISCHIO RESIDUO
		Modifica accidentale dei dati. Cancellazione accidentale dei dati. Inoltro di dati a soggetti non autorizzati a conoscerli.						
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,	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
		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 saranno effettuate a 6 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 " **PNNR-POC-2023-12378113**", 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.