Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI

DATA PROTECTION IMPACT ASSESSMENT
**ESTRATTO**

ID DELLO STUDIO: 6864

PRINCIPAL INVESTIGATOR: PROF. FRANCESCO FANFANI

04/09/2025

## Sommario





E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI

## 1. CONSIDERAZIONI PRELIMINARI

Questo modello di DPIA è implementato dalla Fondazione Policlinico Gemelli IRCSS esclusivamente per adempiere a quanto previsto nell'art. 44 comma 1 bis della legge 29 aprile 2024, n. 56: oggetto di questo modello di DPIA sono gli studi clinici retrospettivi che ricadono nella seguente fattispecie.

L'art. 44 comma 1 bis della legge 29 aprile 2024, n. 56 ha modificato l'art. 110 del Codice della privacy eliminando il requisito dell'autorizzazione preventiva del Garante, ove, per finalità di ricerca medico – scientifica, sia necessario utilizzare dei dati per i quali non è più possibile ottenere il consenso. Il nuovo art. 110 del Codice della privacy, infatti, prevede che: "Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice".

In attuazione del precetto normativo, così come emendato, il Garante ha previsto che nei casi in cui si effettui il trattamento di dati sanitari per fini di ricerca scientifica riferibili a soggetti deceduti o non contattabili per specifici motivi etici o organizzativi si debbano applicare le seguenti garanzie:

- Il titolare deve adottare tutte le misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'Interessato;

- Il titolare deve acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca;

- Il titolare deve accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche o organizzative per le quali informare gli interessati, e quindi acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, se del caso documentando i ragionevoli sforzi effettuati per tentare di contattarli;

- Il titolare deve svolgere e pubblicare la valutazione di impatto, dandone comunicazione al Garante. (cfr newsletter 9.05.2024 n. 298 punto 2).



E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI

## 2. DESCRIZIONE DELLO STUDIO - Contesto, responsabilità, standard, risorse di supporto

### 2.1 SPECIFICARE ID E TITOLO ORIGINALE DELLO STUDIO

Studio RIDER

ID: 6864

Studio no-profit co-finanziato da fondi PNRR Next-Generation EU

PNRR-MCNT2-2023-12378360

Titolo: “Utilizzo della radiogenomica per supportare e migliorare i trattamenti di precisione guidati da biomarkers nel trattamento dei tumori epiteliali confinanti all’utero”

Title: “Radiogenomics to support and implement biomarkers guided delivery of precision medicine in uterine confined endometrial cancer”

### 2.2 SINOSSI DELLO STUDIO

Lo studio RIDER dal titolo “Utilizzo della radiogenomica per supportare e migliorare i trattamenti di precisione guidati da biomarkers nel trattamento dei tumori epiteliali confinati all’utero” ha come obbiettivo quello di valutare il ruolo degli approcci di Intelligenza Artificiale (AI) che combinano immagini e biomarcatori molecolari (dati radiomici e genomici) per stratificare meglio i gruppi di rischio dei pazienti con cancro endometriale ed aiutare i clinici nel processo decisionale terapeutico con un approccio personalizzato. Questa gestione individualizzata identificherà quali pazienti trarranno beneficio da trattamenti specifici, risparmiando agli altri pazienti e al Servizio Sanitario Nazionale la tossicità clinica e finanziaria di terapie inefficaci ed inutili. E’ uno studio multicentrico, osservazionale, esclusivamente retrospettivo, con analisi secondaria dei dati clinici. La Fondazione Policlinico Universitario A. Gemelli IRCCS rappresenta, sotto la conduzione del PI Prof. Francesco Fanfani, il centro promotore dello studio, studio che vede come centro satellite l’Ospedale Civico ARNAS di Cristina Benfratelli di Palermo, con PI il Professor Vito Chiantera. La popolazione target comprende pazienti affette da carcinoma endometriale e trattate con staging chirurgico completo dal 01/01/2017 al 30/08/2024. Lo studio ha una durata di 24 mesi dal 30 Agosto 2024, e prevede di arruolare 1900 pazienti retrospettive. Lo studio prevede il coinvolgimento di diverse Facility quali:

- Genomica
- Immunoistochimica
- Radiomica
- Computational Pathology
- Data Collection



E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI

| | |
|---|---|
| **Titolo** | **Utilizzo della radiogenomica per supportare e migliorare i trattamenti di precisione guidati da biomarkers nel trattamento dei tumori epiteliali confinati all'utero.** |
| **ACRONIMO** | RIDER |
| **PROMOTORE** | Fondazione Policlinico Universitario A. Gemelli, IRCCS<br>L.go Francesco Vito 1, 00168 Roma |
| **Cofinanziatore** | Ministero della Salute – PNRR MCNT2-2023-12378360 |
| **Principal Investigator** | Prof. Fanfani Francesco<br>UOC Ginecologia Oncologica |
| **Sub- Investigator** | Prof.ssa E. Sala<br>Dott. Emanuele Perrone |
| **Background** | Il carcinoma endometriale (CE) è il tumore ginecologico più comune e presenta tassi crescenti di incidenza e mortalità. The Cancer Genome Atlas (TCGA) ha definito quattro diversi sottogruppi molecolari correlati ai comportamenti clinici: i tumori con mutazione POLE (9%) presentano la prognosi migliore, i sottogruppi con deficit di mismatch repair (dMMR) (28%) e p53 wt (50%) (profilo molecolare non specifico, NSMP) hanno una prognosi intermedia, mentre quelli con mutazione p53 (12%) hanno i risultati peggiori.[1-2]<br><br>La radiogenomica sta assumendo un ruolo sempre più rilevante nella stratificazione dei gruppi di rischio prognostico. In un recente studio, il nostro gruppo di ricerca ha creato e validato modelli radiomici applicati alle immagini ecografiche, in grado di identificare il gruppo ad alto rischio di CE.[3]<br><br>L'ipotesi della nostra ricerca è valutare il ruolo degli approcci di Intelligenza Artificiale (AI) che combinano immagini e biomarcatori molecolari (dati radiomici e genomici) |



E-MAIL: dpo@policlinicogemelli.it

| | |
|---|---|
| | per stratificare meglio i gruppi di rischio dei pazienti con cancro endometriale e aiutare i clinici nel processo decisionale terapeutico con un approccio personalizzato. Questa gestione individualizzata identificherà quali pazienti trarranno beneficio da trattamenti specifici, risparmiando agli altri pazienti e al Servizio Sanitario Nazionale la tossicità clinica e finanziaria di terapie inefficaci e inutili. |
| **Obiettivo** | Con il presente studio intendiamo integrare nuovi biomarcatori molecolari e approcci guidati dall'intelligenza artificiale (IA), combinando immagini e dati molecolari per stratificare meglio i gruppi di rischio dei pazienti con CE. Nello specifico:<br>- **Obiettivo 1: Valutare l'impatto di ulteriori caratteristiche molecolari, come l'invasione degli spazi linfovascolari (LVS), l'espressione dei recettori per estrogeni e progesterone (ER/PR), L1CAM e CTNNB1 sulla prognosi del CE NSMP.**<br>- **Obiettivo 2: Esplorare le differenze prognostiche nei sottotipi dMMR.**<br>- **Obiettivo specifico 3A: Valutare l'impatto prognostico delle mutazioni POLE al di fuori delle regioni hotspot utilizzando un punteggio di patogenicità POLE.**<br>- **Obiettivo 3B: Identificare una firma radiogenomica per prevedere la prognosi delle classi di rischio molecolare del CE.** |
| **Disegno dello studio** | Il presente è uno studio multicentrico osservazionale retrospettivo. |
| **Popolazione Target** | Pazienti affette da CE e trattate con staging chirurgico completo dal 01/01/2017 a 30/08/2024 presso la Fondazione Policlinico Universitario A. Gemelli, IRCCS e Ospedale ARNAS Civico di Cristina Benfratelli (Palermo). |
| **Endpoint primario** | Endpoint primario di questo studio, per gli obiettivi individuati, è la sopravvivenza libera da recidiva (RFS). |

| | |
|---|---|
| **Endpoint secondario** | Endpoint secondario è la sopravvivenza complessiva (OS) |
| **Criteri di inclusione** | • Pazienti affette da qualsiasi stadio FIGO e grado dei CE sottoposte a staging chirurgico primario completo dal 01/01/2017 a 30/08/2024 |
| **Criteri di esclusione** | • CE non epiteliali (ad esempio, leiomiosarcoma, rabdomiosarcoma)<br>• Pazienti affette da tumori maligni sincroni<br>• Pazienti che hanno ricevuto trattamento neoadiuvante. |
| **Durata dello studio** | Lo studio durerà 24 mesi dall'approvazione del presente Protocollo da parte del Comitato Etico. |
| **Numero di pazienti** | 1900 |
| **Piano Statistico (dimensionamento del campione ed analisi dei dati)** | **Obiettivo 1**: Secondo la disponibilità di pazienti registrati, consideriamo circa 1.000 pazienti con EC NSMP. Questi numeri si basano sui nostri dati preliminari disponibili nel nostro database chirurgico prospettico interno mantenuto in REDCap. L'intento principale è costruire un nomogramma basato su caratteristiche cliniche e molecolari per prevedere la RFS. Il numero di eventi per RFS registrati finora è 58. Questo numero di eventi, utilizzando la regola pratica di 10 eventi per variabile, consentirà di considerare circa 6 fattori nel nomogramma.<br>**Obiettivo 2**: Secondo la disponibilità di pazienti registrati, consideriamo circa 500 pazienti con EC MMR-d. Questi numeri si basano sui nostri dati preliminari disponibili nel nostro database chirurgico prospettico interno mantenuto in REDCap. L'outcome primario sarà la RFS, mentre l'OS sarà l'outcome secondario. L'intento principale è definire se specifici fenotipi MMR-d valutati tramite IHC, lo stato di metilazione del promotore di MLH1 o la presenza della Sindrome di Lynch/simile Lynch siano associati a un diverso rischio di RFS e OS. Il numero di eventi per RFS registrati finora è 34. |

| | |
|---|---|
| | Per l'obiettivo 1 e 2 le statistiche descrittive saranno utilizzate per illustrare la distribuzione di ciascun fattore. Le associazioni tra caratteristiche cliniche di base e caratteristiche molecolari saranno descritte utilizzando il test $\chi^2$ o il test esatto di Fisher (per le variabili categoriali) e il test t o il test di Mann-Whitney (per le variabili continue), a seconda del caso. L'OS e la RFS saranno calcolate in mesi dalla data della diagnosi al primo evento, includendo la data dell'ultimo follow-up o del decesso (OS) e/o della recidiva (RFS). L'OS e la RFS saranno stimate utilizzando il metodo di Kaplan-Meier e le curve di sopravvivenza saranno confrontate mediante il test del log-rank. Le variabili saranno indagate tramite il modello di Cox a rischi proporzionali per valutarne il valore prognostico. Le variabili associate a un valore $p < 0,05$ nella regressione semplice saranno incluse nella regressione multipla. Ogni modello sarà verificato per le ipotesi di proporzionalità esaminando i residui di Schoenfeld.<br>Infine, sarà prodotto un nomogramma, e verrà realizzato un grafico di calibrazione basato sulle probabilità previste ed effettive, oltre al calcolo dell'indice C per valutare l'accuratezza nella previsione. Verrà implementata una validazione interna del modello basata su una cross-validation k-fold, e la procedura sarà ripetuta un gran numero di volte per ottenere un indice di concordanza corretto per il bias.<br><br>**Obiettivo 3A**: In base ai pazienti disponibili, consideriamo circa 400 pazienti con CE POLE mutato. Verrà sviluppato un sistema di punteggio per classificare le nuove varianti di POLE, tenendo in considerazione le sostituzioni nucleotidiche (come C>A, C>G, T>G), la frequenza degli indel, il TMB e la presenza di mutazioni ricorrenti. Questo sistema di punteggio mira a valutare la patogenicità delle mutazioni e fornire una migliore stratificazione dei pazienti basata su queste diverse alterazioni genomiche. Le statistiche descrittive saranno utilizzate per illustrare la distribuzione di ciascun fattore, utilizzato per calcolare il punteggio. Per la creazione del punteggio, verrà effettuato un confronto tra pazienti con mutazioni POLE |

| | |
|---|---|
| | benigne e pazienti con mutazioni hotspot mediante test t, test di Mann-Whitney o test $\chi^2$, a seconda del caso.<br><br>**Obiettivo 3B**: Circa 400 pazienti saranno analizzati con l'obiettivo di prevedere le classi di rischio molecolare degli EC con un modello radiomico. Questa dimensione del campione consentirà di considerare 6 predittori per raggiungere un errore medio assoluto di previsione di 0,05. L'AUC dei modelli sarà calcolata per ciascuna categoria dicotomizzando le classi di rischio EC (due possibili AUC). Gli intervalli di confidenza dell'AUC saranno fissati al livello del 97,5% per tenere conto del doppio calcolo e, assumendo un'AUC di circa 0,80, avranno una semi-ampiezza di 0,05. Saranno implementate diverse strategie di selezione delle caratteristiche per ridurre la dimensionalità delle caratteristiche radiomiche. Questo includerà l'analisi univariata tramite il test di Mann-Whitney o il test di Kruskal-Wallis, secondo il caso, per valutare l'associazione tra le caratteristiche e le classi di rischio, l'analisi della robustezza delle caratteristiche rispetto ai parametri di acquisizione delle immagini, l'analisi di correlazione tra le caratteristiche per rimuovere la collinearità ed evitare l'overfitting, l'algoritmo Boruta e l'analisi delle componenti principali. Saranno sviluppati modelli predittivi basati sulle caratteristiche radiomiche selezionate, derivate da US e MRI. Saranno implementati diversi modelli di machine learning con complessità crescente utilizzando le caratteristiche radiomiche selezionate: regressione logistica con diverse penalizzazioni, foresta casuale, alberi di boosting a gradiente, macchina a vettori di supporto. Il modello con le migliori prestazioni sarà selezionato in base all'area sotto la curva (AUC) della curva ROC (Receiver Operating Characteristic). Inoltre, le prestazioni del modello saranno valutate utilizzando le statistiche della matrice di confusione, inclusi accuratezza, sensibilità, specificità, valore predittivo positivo e negativo, calcolati utilizzando una soglia definita dal metodo dell'indice di Youden. La calibrazione del modello sarà valutata utilizzando grafici di calibrazione che confrontano eventi previsti ed effettivi. Saranno sviluppati modelli predittivi basati su caratteristiche di deep learning estratte dalle immagini H&E. Il |

| | |
|---|---|
| | modello con le migliori prestazioni sarà selezionato utilizzando AUC, accuratezza, sensibilità, specificità e F1-score. |
| **SICUREZZA/GESTIONE REGOLATORIA DEGLI EVENTI AVVERSI** | Trattandosi di uno studio osservazionale retrospettivo con analisi secondaria dei dati, non- sussiste obbligo attuale di segnalazione di sospette reazioni avverse, essendo state eventualmente le stesse già a suo tempo comunicate secondo quanto previsto da DM 30.04.2015 e GVP modulo VI sez. C.1.2.1.2.<br><br>I dati personali dei soggetti coinvolti nel protocollo non saranno utilizzati per scopi di profilazione né per prendere decisioni automatizzate che possano comportare un rischio significativo per gli stessi. Tutti i processi automatizzati sono sotto controllo umano. |
| **DOCUMENTO DI RIFERIMENTO PER LA SICUREZZA** | Il presente studio è classificato come osservazionale retrospettivo con analisi secondaria dei dati clinici, pertanto non vi è alcun ulteriore requisito per la presentazione di ADR (Adverse Drug Reaction) all'Autorità Nazionale Competente in quanto tutti gli obblighi di segnalazione sono stati adempiuti al momento della presentazione dell'ADR come da normativa applicabile (DM 30.04.2015 e GVP, Good Vigilance Practice, modulo VI, sezione C 1.2.1.2.). |
| **Bibliografia** | 1 Perrone E, De Felice F, Capasso I, Distefano E, Lorusso D, Nero C, Arciuolo D, Zannoni GF, Scambia G, Fanfani F. The immunohistochemical molecular risk classification in endometrial cancer: A pragmatic and high-reproducibility method. Gynecol Oncol. 2022 Jun;165(3):585-593. doi: 10.1016/j.ygyno.2022.03.009. Epub 2022 Mar 24. PMID: 35341588.pragmatic and high-reproducibility method. Gynecol Oncol. 2022 Jun;165(3):585-593. doi: 10.1016/j.ygyno.2022.03.009. Epub 2022 Mar 24. PMID: 35341588.<br><br>2 Perrone E, Capasso I, De Felice F, Giannarelli D, Dinoi G, Petrecca A, Palmieri L, Foresta A, Nero C, Arciuolo D, Lorusso D, Zannoni GF, Scambia G, Fanfani F. Back to the future: The impact of oestrogen receptor profile in the era of molecular endometrial cancer classification. Eur J Cancer. 2023 Jun;186:98-112. doi: 10.1016/j.ejca.2023.03.016. Epub 2023 Mar 22. PMID: 37062213.<br><br>3 Moro F, Albanese M, Boldrini L, Chiappa V, Lenkowicz J, Bertolina F, Mascilini F, Moroni R, Gambacorta MA, Raspagliesi F, Scambia G, Testa AC, Fanfani F. Developing and validating ultrasound-based radiomics models for predicting high-risk endometrial cancer. Ultrasound Obstet Gynecol. 2022 Aug;60(2):256-268. doi: 10.1002/uog.24805. PMID: 34714568. |

## 2.3 TIPOLOGIA DI STUDIO

- Multicentrico
- No-profit[1]

Specificare se retrospettivo:
☒ SI

## 2.4 NUMERO DI PAZIENTI ARRUOLATI

1900 pazienti da arruolare in totale tra i due centri.

## 2.5 DATASET, PSEUDONIMIZZAZIONE, CONTROLLI DI INTEGRITÀ, DATA BREACH

- Riportare una riga di dataset (es. CRF)

Riportata in allegato Dati pazienti eCRF lista.xs

- Produrre un esempio della pseudonimizzazione utilizzata per lo Studio (se non possibile riportare la modalità di pseudonimizzazione)

1) I dati raccolti dei partecipanti agli studi sono pseudonimizzati attraverso l'utilizzo di un ID univoco generato automaticamente da REDCap, che non contiene alcuna informazione direttamente riconducibile al paziente.
Il collegamento tra l'ID REDCap e l'identità del paziente è possibile solo tramite il codice sanitario, che rappresenta l'identificativo univoco utilizzato all'interno del nostro istituto.
Tuttavia, il codice sanitario, pur essendo tecnicamente un dato identificativo, non consente l'identificazione diretta da parte di soggetti esterni, in quanto può essere associato al paziente solo tramite l'accesso al sistema informativo clinico TrakCare, accesso che è riservato esclusivamente al personale autorizzato dell'ospedale e tramite connessione sicura, tracciata e controllata.
2) Qualora necessario e richiesto dal PI, è possibile raccogliere dati identificativi del paziente che vengono archiviati separatamente sia logicamente sia fisicamente dai dati clinici raccolti durante lo studio.

[1] In caso di No-profit Non co-finanziato Multicentrico, si prega di sottomettere al Comitato Etico anche eventuali contratti tra le parti (es. Data Transfer Agreement).


E-MAIL: dpo@policlinicogemelli.it

Tale separazione è gestita in modo automatizzato attraverso l'utilizzo di un modulo esterno sviluppato ad hoc da personale dedicato della Facility DC e integrato nella piattaforma REDCap (FPG Record Sensitive Data). Questo modulo consente, al momento dell'inserimento dei dati, di archiviare automaticamente eventuali dati identificativi che necessitano di essere raccolti in un **database** separato rispetto ai dati clinici, crittografati e accessibili solo ad utenti con particolari permessi/privilegi qui elencati:

• Selezione del Data Access Groups presente nella configurazione del modulo esterno
• Ruolo PI sempre abilitato.

Questa configurazione è coerente con quanto previsto:

• dall'art. 89 del GDPR, che consente il trattamento di dati particolari per finalità di ricerca scientifica, subordinandolo all'adozione di misure tecniche e organizzative adeguate;
• dalle ICH-GCP, che richiedono che l'identità dei soggetti non sia direttamente accessibile al promotore o a terzi non autorizzati;
• dalle linee guida del Garante per la protezione dei dati personali e dalle indicazioni dell'AIFA –Ufficio Ispezioni GCP, che ribadiscono la necessità di limitare la diffusione dei dati identificativi, garantire la tracciabilità dei trattamenti e implementare misure di sicurezza quali:
• la separazione logica e fisica dei dati;
• la pseudonimizzazione;
• il controllo degli accessi;
• la cifratura dei dati

la valutazione d'impatto (DPIA) nei casi previsti;

• e la formazione del personale coinvolto.

I dati che il modulo gestisce al momento sono i seguenti:

• Nome
• Cognome
• Data di nascita
• Email
• Numero di telefono

Quando l'utente, che ha i permessi/privilegi necessari, si trova ad aggiungere un nuovo record sulla eCRF, o quando si trova sul primo "instrument" della stessa, qualora non siano già stati inseriti i dati sensibili, si visualizza tramite un pop-up una machera che permette di inserire le informazioni sopra citate.

Il modulo crea anche un pulsante sulla eCRF che consente, all'utente con i permessi/privilegi, di visualizzare i dati inseriti precedentemente.

Una volta salvati i dati tramite la maschera, vengono codificati con la crittografia: AES-128-CTR e con una chiave preimpostata, successivamente vengono caricati all'interno di un database dedicato, dove è presente una tabella per la loro archiviazione.

In questo modo i dati non sono più in chiaro e possono essere visualizzati solo attraverso la decodifica con la chiave preimpostata ed esclusivamente per gli utenti con i diritti sopra citati.

- La tabella di conversione è conservata in un luogo/software separato rispetto al dato

1) Nel caso di pseudoanonimizzazione, sia l'ID REDCap sia il codice sanitario del paziente sono registrati all'interno del database REDCap. Tuttavia, il collegamento tra il codice sanitario e l'identità del paziente è possibile solo tramite il sistema clinico TrakCare, accessibile esclusivamente da personale autorizzato dell'ospedale. Pertanto, la "tabella di conversione" tra dato pseudonimizzato e identità del paziente non è contenuta in REDCap, ma è implicita e custodita all'interno di TrakCare, garantendo la separazione logica tra i dati clinici e identificativi.
2) Nel caso di registrazione di dati sensibili (nome, cognome, data di nascita completa, email, numero di telefono) attraverso l'utilizzo del modulo FPG Record Sensitive Data la "tabella di conversione" è ospitata su un server diverso dal server che ospita il database dei dati clinici, i dati sensibili sono codificati con la crittografia: AES-128-CTR e con una chiave preimpostata e possono essere visualizzati solo attraverso la decodifica con la chiave preimpostata ed esclusivamente per gli utenti con i diritti sopra citati

- Come avvengono i controlli per l'esattezza e l'aggiornamento dei dati (integrità del dato)?

I dati vengono inseriti manualmente in REDCap da personale dedicato e da una task force di clinici appositamente formata. Per garantire l'integrità del dato, vengono adottate le seguenti misure:
Controlli incrociati tra fonti cliniche (es. cartella elettronica, referti) prima dell'inserimento.
Validazioni automatiche in REDCap (es. range di valori, campi obbligatori, formati predefiniti).
Revisione periodica dei dati inseriti da parte di un supervisore o data manager.
Aggiornamenti effettuati solo da personale autorizzato, con tracciabilità delle modifiche tramite il sistema di audit trail di REDCap.
Queste procedure assicurano che i dati siano accurati, coerenti e aggiornati, in linea con i requisiti di qualità per gli studi clinici.

- Il PI ha edotto il personale coinvolto nello studio sui comportamenti da tenere in caso di violazione, anche presunta, dei dati personali (data breach)? (specificare la modalità)

Sì. Il Principal Investigator (PI) ha provveduto a istruire in modo esaustivo tutto il personale coinvolto nello studio in merito ai comportamenti da adottare in caso di violazione, anche presunta, dei dati personali (data breach). La formazione è stata erogata attraverso una sessione dedicata durante la Site Initiation Visit (SIV), integrata da un modulo formativo specifico sui principi del GDPR, sulle misure di sicurezza adottate nello studio e sulle modalità di segnalazione e gestione delle violazioni.
Durante il training sono stati illustrati:
Le definizioni di data breach (accesso non autorizzato, perdita, modifica, divulgazione o distruzione accidentale o illecita dei dati);

Le procedure da seguire in caso di sospetta violazione, inclusa la notifica immediata al PI e al Data Protection Officer (DPO) dell'istituto;
I tempi di notifica previsti dalla normativa (entro 72 ore dalla scoperta del data breach);
I canali ufficiali di comunicazione interna per la segnalazione;
Le responsabilità individuali e collettive in materia di protezione dei dati personali.
Infine, il PI ha previsto richiami periodici delle procedure di sicurezza durante le riunioni di avanzamento studio, per garantire il costante aggiornamento e la consapevolezza del team sul tema della sicurezza dei dati.

## 2.6 DATABASE E SOFTWARE UTILIZZATI

- Indicare i database aziendali utilizzati per raccogliere i dati da utilizzare per lo Studio (es: PACS, TrakCare, etc)

  TrakCare, Digistat, PACS, Armonia.

- Per lo studio è necessario utilizzare il/i software/dispositivi/piattaforme online:

| | Nome software/dispositivo/piattaforma | Funzione/utilizzo | Indicare se il Software è installato in FPG o in cloud | Indicare il Fornitore /o indicare se open source |
|---|---|---|---|---|
| 1 | TrakCare | Dati clinici, cartella clinica elettronica | FPG | Intersystems |
| 2 | RedCap | eCRF | FPG | software gratuito per la raccolta e la gestione dati, sviluppato e fornito da Vanderbilt University (non è open source). |
| 3 | cBioportal | Gestione dei dati genomici | FPG | open |



E-MAIL: dpo@policlinicogemelli.it

| | | | | |
|---|---|---|---|---|
| 4 | 3D Slicer | Visualizzazione e contornazione MRI | FPG | open |
| 5 | ITK-Snap | Visualizzazione e contornazione MRI | FPG | open |
| 6 | Aliza Medical Imaging | Visualizzazione e contornazione US | FPG | open |
| 7 | RStudio | Analisi dati/immagini e modellistica | FPG | open |
| 8 | Visual Studio Code | Editor utilizzato per creazione linguaggio di programmazione Python per elaborazione immagini | FPG | open |
| 9 | Slide Viewer | Visualizzazione vetrini digitalizzati | FPG | open |
| 10 | QuPath | Analisi immagini istopatologiche digitali | FPG | open |
| 11 | MODDICOM | Contornazione immagini | FPG | open |

## 2.7 CRF/ECRF

- In caso di eCRF indicare software/piattaforma utilizzata
  Redcap Research Electronic Data Capture

  Il software utilizzato per la raccolta e gestione dei dati è REDCap, una piattaforma sviluppata dalla Vanderbilt University e distribuita con licenza gratuita per scopi non commerciali. Nel nostro caso, REDCap è ospitato e gestito internamente dalla Fondazione, che ne cura l'installazione, la configurazione e la manutenzione. Pertanto, non si tratta di un servizio in outsourcing, ma di una piattaforma gestita direttamente dall'ente

- Indicare modalità di scambio dei files provenienti dai centri di sperimentazione (caso multicentrico)

Nel caso di studi multicentrici, non è previsto lo scambio di file tra i centri satellite e FPG. Ogni centro partecipante accede direttamente alla piattaforma REDCap tramite connessione sicura e compila online la eCRF. L'accesso alla piattaforma avviene tramite autenticazione a due fattori (2FA), con invio di un codice OTP via email. Inoltre, ogni centro ha accesso esclusivamente ai dati da esso inseriti, grazie alla configurazione dei permessi utente in REDCap, che garantisce la riservatezza e la compartimentazione dei dati tra i centri.

- Nel caso di CRF (cartaceo): indicare modalità di conservazione dei documenti cartacei e (nel caso di studi multicentrici) le modalità di trasmissione dai Centri alla Fondazione

  I documenti sono archiviati in locali sicuri presso ciascun centro, in armadi chiusi a chiave e accessibili solo al personale autorizzato.

La trasmissione alla Fondazione, se prevista, avviene tramite spedizione tracciata (es. corriere o posta raccomandata) o consegna diretta.
Una volta ricevuti, i documenti sono conservati in archivio fisico protetto presso la Fondazione.
In ogni caso, i dati contenuti nei documenti cartacei vengono trascritti nella eCRF REDCap da personale autorizzato, garantendo così la digitalizzazione e la tracciabilità delle informazioni.

## 2.8 RISORSE: SOGGETTI INTERNI COINVOLTI NELLO STUDIO (RUOLI E FUNZIONI)

Tutti i soggetti che tratteranno i dati personali sono stati nominati come da Istruzione Operativa - IO.018
☒ SI
☐ NO

## 2.9 RUOLI PRIVACY

- **Titolare del Trattamento** (Promotore): Fondazione Policlinico Universitario Agostino Gemelli IRCCS Largo Francesco Vito, n. 1 – 00168 Roma.

- **Eventuali autonomi titolari** ☒ SI ☐ NO

| Autonomi titolari | Indirizzo |
|---|---|

| | | |
|---|---|---|
| 1 | Policlinico Gemelli IRCCS (centro di sper.) | Largo F. Vito 8, Roma. |
| 2 | Azienda Osp Pol. Un. G. Martino (centro di sper.) | Messina |
| 3 | Università Federico II (centro di sper.) | Napoli |

- **Eventuali responsabili del trattamento** ex art. 28 GDPR

- **Eventuali responsabili del trattamento** ex art. 28 GDPR

  - Deposito campioni biologici presso biobanche esterne/biorepository ☒ SI ☐ NO

| | Nome laboratorio | Indirizzo |
|---|---|---|
| 1 | Dipartimento di Oncologia e Medicina Molecolare, Istituto Superiore di Sanità | Viale Regina Elena 299, 00168 Roma |

  - Corrieri e trasportatori di materiale biologico, dataset contenuti in supporti fisici, etc ☐ SI ☒ NO

| | Nome Fornitore | Indirizzo |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

  - Fornitori/gestori/manutentori di applicativi/software outsourcing (es. eCRF, Diario elettronico, APP di monitoraggio, APP/Software collegabili a dispositivi indossabili connessi, televisita/telemedicina, piattaforme online)

| | Nome software/dispositivo | Fornitore | Indirizzo |
|---|---|---|---|
| 1 | GARR filesender | Consortium GARR | Via dei Tizii,6 - 00185 Roma, Italia |

  - Contract Research Organization (CRO) ☐ SI ☒ NO



E-MAIL: dpo@policlinicogemelli.it

Se sì, specificare Nome e indirizzo della CRO

- Ulteriori eventuali responsabili del trattamento ☐ SI ☒ NO

| | Altri | Indirizzo |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

### 2.10 TRASFERIMENTI DATI EXTRA UE

I dati sono trasferiti extra UE

☐ SI ☒ NO

## 3. PRINCIPI FONDAMENTALI

### 3.1 PROPORZIONALITÀ E NECESSITÀ

### 3.11 Gli scopi del trattamento sono specifici, espliciti e legittimi?

Sì, il trattamento è eseguito per la finalità di ricerca scientifica in ambito medico/sanitario e nei limiti strettamente funzionali al perseguimento di tale finalità.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |



E-MAIL: dpo@policlinicogemelli.it

### 3.12 Quali sono le basi legali che rendono lecito il trattamento?

Norma di legge Art. 110 bis D.lgs n. 196/2003 e ss. mm. ii (Codice Privacy) in conformità degli articoli 9 lett J e 89 GDPR.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

### 3.13 Ci sono standard applicabili al trattamento?

Gov e PRO

- REG:016 Rev:1.0 01/03/2024 (REGOLAMENTO RICERCA CLINICA)
- PRO.1049 PROCEDURA: Gestione delle Informative e dei Consensi Adempimenti in Materia di Protezione dei Dati Personali
- IO.018 Istruzione operativa: Data Privacy Manager, Data Privacy Manager Assistant e Incaricati Del Trattamento
- PRO.021: Procedura Gestione della Documentazione Sanitaria in Ospedale
- Nomine autorizzato al trattamento
- MAN 014: Manuale per l'Utilizzo per le Procedure Informatiche

La Ricerca Clinica è inoltre regolamentata dalla seguente normativa, da Standard Nazionali e Internazionali:

- Convenzione del Consiglio d'Europa per la protezione dei diritti dell'uomo e della dignità dell'essere umano (Convenzione di Oviedo del 04/04/1997, ratifica autorizzata con Legge 28/03/2001 n. 145);
- Declaration of Helsinki (World Medical Association) "Ethical Principles for Medical Research Involving Human Subjects" del 1964 e ss.mm.ii;
- D.lgs 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e ss.mm.ii.
- D.lgs 30 dicembre 1992, n. 502, recante riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421;

- D.M. Ministero della Salute 30 novembre 2021: Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52.
- D.M. Ministero della Salute 1° febbraio 2022: Individuazione dei comitati etici a valenza nazionale.
- d.M. Ministero della Salute 26 gennaio 2023: Individuazione di quaranta comitati etici territoriali.
- Linee guida di buona pratica clinica (Good Clinical Practice - GCP) e ss. mm.ii adottate dall'Unione Europea nel 1996, recepite nell'ordinamento italiano con D.M. 15 luglio 1997, n.162; ICH E6 (R3) GOOD CLINICAL PRACTICE GCP (luglio 2025)
- Linee guida "Per i trattamenti di dati personali del Garante per la Protezione dati personali nell'ambito delle sperimentazioni cliniche di medicinali" del 24 luglio 2008
- Regolamento (UE) n. 536/2014 del Parlamento Europeo e del consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE;
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR) che abroga la direttiva 95/46/CE;
- Regolamento (UE) n 2017/745 del Parlamento Europeo e del Consiglio del 5 aprile 2017 relativo ai dispositivi medici;
- Regolamento (UE) n 2017/746 del Parlamento Europeo relativo ai dispositivi medico diagnostici in vitro;
- Autorizzazione Generale del 22/2/2017 e ss modifiche (Autorizzazione Generale al trattamento di dati genetici);

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

### 3.14 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 avviene nel rispetto del principio di minimizzazione in quanto sono raccolti e trattati solo i dati strettamente necessari per il raggiungimento delle finalità dello Studio, come indicato nel Protocollo approvato dal Comitato Etico.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|



E-MAIL: dpo@policlinicogemelli.it

| | | | | |
|---|---|---|---|---|
| | X | | | |

### 3.15 I dati sono esatti e aggiornati?

Il trattamento dei dati personali avviene in conformità del Protocollo dello Studio approvato dal Comitato Etico e nel rispetto dei principi di buona pratica clinica (GCP) a garanzia dell'esattezza dei dati raccolti e della non alterazione dei dati stessi; i dati sono costantemente aggiornati e fedelmente riportati nelle Schede Raccolta Dati cartacee (Case Report Forms –CRF) o elettroniche (electronics Case Report Forms- eCRF). Tutti i documenti essenziali sono raccolti nel Trial Master File (TMF) che è il fascicolo permanente della sperimentazione che consente di verificare in ogni momento come essa viene condotta e la qualità dei dati ottenuti. L'accesso ai dati necessari per lo studio è consentito solo al personale espressamente autorizzato che opera sotto la vigilanza del Medico Sperimentatore (Principal Investigator –PI); ogni accesso alle eCRF e al TMF è tracciato.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

### 3.16 Qual è il periodo di conservazione dei dati?

I dati e i campioni biologici sono conservati per un arco di tempo non superiore a quello necessario per conseguire le finalità per le quali sono stati raccolti e trattati (art. 11, comma 1, lett. e) del Codice Privacy, il termine massimo di conservazione è di 7 anni dal termine dello studio, come da Provvedimento Autorità Garante del 18 luglio 2023 [9920977] "Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008 " che ha ritenuto congruo il termine di 7 anni desunto dall'art. 18 del D. Lgs. 6 novembre 2007, n. 200 (Attuazione della direttiva 2005/28/CE recante principi e linee guida dettagliate per la buona pratica clinica relativa ai medicinali in fase di sperimentazione a uso umano).

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

## 3.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore



### 3.21 Come sono informati del trattamento gli interessati?

Gli interessati sono informati tramite Informativa compilata a cura del Titolare (art. 13 GDPR) e pubblicata sul sito aziendale nella sezione del sito: https://www.policlinicogemelli.it/servizi-paziente/privacy-e-protezione-dei-dati-personali/.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

### 3.22 Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile. La presente DPIA consente di derogare all'acquisizione del consenso ai sensi dell'art 110 bis D.lgs. 30 giugno 2003, n. 196 come novellato dall'art. 44 comma 1 bis della legge 29 aprile 2024, n. 56.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

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

Nella informativa pubblicata sul sito sono fornite agli interessati specifiche indicazioni per esercitare il diritto di accesso e gli altri diritti riconosciuti dal GDPR, con indicazione dei dati di contatto del Titolare e del DPO aziendale. L'esercizio dei diritti degli interessati può essere suscettibile di limitazioni in considerazione della finalità di ricerca scientifica nei limiti ed alle condizioni indicate dall'art. 89 GDPR. Il diritto alla portabilità dei dati non è applicabile in questo caso poiché la base giuridica del trattamento è una norma di legge (110 bis) e non è basato sul consenso dell'interessato (art. 20 GDPR).

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

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

L'interessato ha il diritto di chiedere al Titolare del trattamento la rettifica e la cancellazione dei dati con le modalità indicate nell'informativa scrivendo ai dati di contatto del Titolare e del DPO aziendale



E-MAIL: dpo@policlinicogemelli.it

indicati nella stessa. Il diritto alla cancellazione può subire delle limitazioni per la finalità di ricerca scientifica in conformità di quanto previsto dall'art. 17, par. 3 lett. d) GDPR.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

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

Nella informativa pubblicata sul sito sono fornite agli interessati specifiche indicazioni per esercitare i diritti riconosciuti dal GDPR, con indicazione dei dati di contatto del Titolare e del DPO aziendale. L'esercizio dei diritti degli interessati può essere suscettibile di limitazioni in considerazione della finalità di ricerca scientifica nei limiti ed alle condizioni indicate dall'art. 89 GDPR.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

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

Gli obblighi dei responsabili del trattamento sono espressamente definiti nell'atto di nomina ex art. 28 GDPR ed anche contrattualizzati con apposito documento nei casi in cui i fornitori vengano a contatto (anche solo potenzialmente) coi dati personali a titolarità della Fondazione (ad esempio: laboratori di analisi esterni, corrieri esterni, fornitori di software provvisti di contratto di manutenzione, etc).

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

### 3.27 In caso di trasferimento di dati al di fuori dell'unione europea, i dati godono di una protezione equivalente?

Il trasferimento è sempre soggetto alla rigorosa osservanza delle condizioni e delle garanzie previste dal Capo V del GDPR (es: decisioni di adeguatezza, SCCs, etc.).

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|---|---|---|---|---|
| | X | | | |

## 4. CALCOLO DEL RISCHIO

Questo capitolo descrive i criteri adottati per calcolare il rischio che il trattamento oggetto di DPIA comporta nell'ambito dei diritti e delle libertà dell'interessato.

Si procede con il calcolo:
- del Rischio Accettabile **RA**
- del Rischio Inerente **RI**
- della % di mitigazione del Rischio Inerente dovuta all'implementazione delle contromisure di sicurezza.
- del **Rischio Residuo** calcolato come Ri – (Ri x % di mitigazione).

Qualora il trattamento sottoposto a DPIA risulti associato ad un valore di Rischio Residuo inferiore al valore di Rischio "Accettabile" (Ra), il trattamento stesso sarà considerato adeguato dal punto di vista della protezione dei dati personali, al netto di un monitoraggio periodico.

Il **rischio accettabile** (Ra) è il valore di rischio che il titolare del trattamento ritiene adeguato al trattamento in oggetto e che pertanto è disposto ad accettare.

Il **rischio inerente** è il rischio che grava su un'organizzazione in assenza di qualsiasi azione o misura in grado di ridurne la Probabilità e/o la Gravità e rappresenta la massima perdita realizzabile in seguito al concretizzarsi dei rischi e alla mancanza di azioni tese a limitarne gli effetti.
Il Rischio Inerente si calcola moltiplicando la Probabilità per la Gravità (o impatto): RI=PxG.

**La probabilità** di realizzazione di un rischio (in termini di protezione del dato personale) è qui considerata sulla base delle caratteristiche del trattamento che possano mettere a repentaglio diritti e libertà degli interessati.
La stima della probabilità di un accadimento avverso avviene attraverso la valutazione dei seguenti elementi: Profilazione, Monitoraggio, Consenso, Complessità del trattamento, Informativa, Nuove Tecnologie, Revisione DPIA, Numero interessati, Data Breach. Ogni elemento presenta quattro scenari diversi ai quali è associato uno score da 1 a 4.
In base alla compilazione della tabella contenente gli elementi succitati si otterrà un punteggio di scoring compreso in un range da 9 a 36.
Associato allo scoring c'è il livello di Probabilità P (Improbabile, Poco Probabile, Probabile, Molto Probabile) col relativo punteggio di P (1-improbabile, 2-poco probabile, 3-probabile, 4-molto probabile).

**La gravità o impatto** rappresenta l'entità del danno in cui potrebbero incorrere gli interessati in quanto persone fisiche al manifestarsi di un rischio legato ad un data breach: tale danno può essere di natura fisica, materiale o immateriale, come da tabella sottostante. Il data breach può concretizzarsi a seguito di una perdita di Riservatezza (R), Integrità (I) e Disponibilità (D) del dato personale.
La stima della gravità di un accadimento avverso avviene attraverso la valutazione dei possibili danni divisi in tre categorie: Fisico (danni fisici subiti dall'interessato), Materiale (danni che coinvolgono le proprietà dell'interessato), Immateriale.


E-MAIL: dpo@policlinicogemelli.it

Ogni categoria presenta quattro scenari diversi ai quali è associato uno score da 1 a 4. In base alla compilazione della tabella si otterrà un punteggio di scoring compreso in un range da 3 a 12. Associato allo scoring c'è il livello di Gravità G (Lieve, Moderata, Grave, Molto Grave) col relativo punteggio di G (1-lieve, 2-moderato, 3-grave, 4-molto grave).

Moltiplicando GxP otteniamo 4 possibili valori di Rischio Inerente: RI (1-lieve, 2-moderato, 3-grave, 4-molto grave)

**Le tabelle delle contromisure** adottate per minimizzare il rischio inerente sono composte da varie voci, ognuna delle quali associata ad un valore di adeguatezza (da 0 – non applicabile a 3 - adeguato). Tali valori di adeguatezza concorrono a generare la % di abbattimento del rischio.

Il Rischio Residuo finale si calcola come RI -RI x %Mitigazione).

## 5. ANALISI DEI RISCHI

### 5.1 Tabella delle Contromisure tecniche

| ID | Misure |
|---|---|
| 1 | I dati dello studio sono trattati tramite software installati su sistemi FPG e di conseguenza protetti dai sistemi e dalle policies di cybersecurity di FPG, che comprendono:<br>• Misure di pseudonimizzazione e crittografia dei dati personali<br>• Misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di elaborazione: firewall perimetrali, proxy, antivirus/antimalware sulle pdl e sui server, blocco delle installazioni sulle pdl, disattivazione automatica schermo, hardening dei sistemi, etc<br>• Misure per garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico; ex backup e procedure di continuità operativa<br>• Procedure per testare, valutare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento: ex effettuazione di VA periodiche<br>• Misure per l'identificazione, l'autorizzazione e la profilazione degli utenti: ex: utenze AD, password policy, eliminazione account inattivi, accesso profilato ai software solo dietro autorizzazione, etc<br>• Misure per la protezione dei dati durante la trasmissione: ex VPN, Autenticazione a più fattori<br>• Misure per la protezione dei dati durante l'archiviazione: ex Crittografia, Backup<br>• Misure per garantire la sicurezza fisica dei luoghi in cui vengono trattati i dati personali: ex badge elettronici di accesso consentono l'accesso agli ingressi comuni dell'edificio. La sicurezza degli ingressi comuni dell'edificio è garantita e gestita dai responsabili dell'edificio e dalle società di vigilanza; l'accesso ai sistemi IT (sala server e sala di archiviazione IT) è limitato al personale autorizzato con accesso tramite badge elettronico, come previsto da procedure specifiche. |



E-MAIL: dpo@policlinicogemelli.it

| | |
|---|---|
| | • Misure per garantire la configurazione del sistema, inclusa la configurazione predefinita: ex. disattivazione e/o modifica utenze di default su server e apparati di rete, gestione utenze di servizio automatizzate;<br>• Misure per garantire una conservazione limitata dei dati. |
| 2 | I dati dello studio sono caricati in cloud gestiti da Fornitori FPG iscritti nell'albo fornitori e provvisti di regolare contratto e atto di nomina a responsabile del trattamento |
| 3 | I software/ Piattaforma fanno parte del Portafoglio Applicativo FPG |
| 4 | La tabella di conversione è conservata in un luogo/software separato rispetto al dato pseudonimizzato |
| 5 | I codici pseudonimizzati rispettano la previsione di non inserire riferimenti identificativi dei pazienti |
| 6 | I dati eventualmente trasmessi all' esterno sono inviati tramite canali protetti/cifrati |
| 7 | L' integrità del dato è garantita da log di accesso e modifica e da periodiche revisioni di tali log |
| 8 | Il trattamento dei dati personali avviene solo tramite dispositivi/ personal computer aziendali |
| 9 | l'accesso al software/piattaforma/piattaforma ECRF contenente i dati avverrà con credenziali personali |
| 10 | La piattaforma ECRF è raggiungibile via protocollo https |
| 11 | Il file contenente le ecrf è cifrato e conservato su dispositivi FPG |
| 12 | I files contenuti nei supporti fisici sono cifrati |
| 13 | Se ai fini dello Studio verranno usati o testati o sviluppati algoritmi di IA si attesta che:<br><br>a) c'è una valutazione del codice utilizzato (ad esempio per vagliare la presenza di backdoor)<br><br>b) tutti i processi automatizzati sono sotto controllo umano: nel ciclo di vita del modello di intelligenza artificiale utilizzato per l'analisi sono previsti meccanismi strutturati di controllo umano (Human Oversight) volti a garantire la correttezza, l'affidabilità e la conformità etico-legale del sistema. |

## 5.2 Tabella delle Contromisure logistiche

| ID | Misure |
|---|---|
| 1 | L'accesso ai luoghi dove sono conservati i dispositivi utilizzati per il trattamento è consentito solo a personale autorizzato |
| 2 | L'accesso ai luoghi dove sono conservati i dati (ad esempio campioni biologici) e/o la documentazione utilizzati per il trattamento è consentito solo a personale autorizzato |
| 3 | L'eventuale documentazione cartacea è conservata in contenitori (armadi, schedari, ecc.) muniti di serratura la cui chiave è nelle disponibilità del solo personale autorizzato. |

## 5.3 Tabella delle Contromisure Organizzative

| ID | Misure | Evidenze |
|---|---|---|
| 1 | Ruoli e responsabilità | Descritte nella IO 0.18 per i soggetti interni e descritte per lo studio in oggetto nei parr.2.7 e 2.8. Per tutti i responsabili ex art. 28 GDPR sono predisposti atti di nomina. |
| 2 | Formazione | Il Titolare attua una specifica attività di formazione per il personale e per i soggetti coinvolti nella gestione del trattamento dei dati personali, al fine di presidiare adeguatamente le istruzioni fornite e, in ogni caso, di promuovere la cultura della privacy e della sicurezza delle persone fisiche con riguardo ai dati personali all'interno dell'organizzazione aziendale.<br>Il corso erogato al personale di FPG si basa sulla normativa vigente sul trattamento dei dati personali delle persone fisiche, ovvero, il Regolamento Europeo (UE) 2016/679 e il Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 2003) modificato e integrato dal D.Lgs. 101/2018.<br>Sono, inoltre, previsti degli specifici eventi formativi, in relazione agli specifici settori di competenza.<br>Sono altresì previste delle apposite indicazioni e linee guida specifiche per gli Studi Clinici. |
| 3 | Gov e PRO | Vedi par. 3.13 della presente DPIA |
| 4 | Gestione data breach | Lo staff coinvolto nello studio è formato in merito alla pro. da adottare al verificarsi di un data breach. |
| 5 | E' presente un apposito spazio aziendale dove pubblicare informativa e DPIA dello studio | Vedi par. 3.22 della presente DPIA |
| 6 | E' ottemperato l'obbligo di invio comunicazione al GPDP tramite PEC aziendale? | Sì con PEC dpo.gemelli@pec.it |

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

| Riservatezza – accesso illegittimo ai dati |
|---|
| Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere:<br>• Perdita di riservatezza dei dati personali protetti da segreto professionale;<br>• Conoscenza da parte di terzi non autorizzati di dati particolari laddove si riesca a re-identificare l'interessato;<br>• rischio di re-identificazione degli interessati/pazienti arruolati per i progetti di ricerca. |
| **Integrità – modifica indesiderata dei dati** |
| Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere:<br>• Perdita del controllo della qualità del dato.<br>• Inoltre, nel caso di modifica indesiderata dei dati, la Fondazione potrebbe incorrere nel rischio di veder vanificate le attività di ricerca. |
| **Disponibilità – perdita dei dati** |
| Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere:<br>• Nessuno sull'interessato, trattandosi di dati copiati dai DB aziendali ai software di ricerca e non utilizzati a fini di cura ma di ricerca. |

## 5.5 Quali sono le principali minacce che potrebbero concretizzare il rischio?

| Riservatezza – accesso illegittimo ai dati |
|---|
| Replica dei dati su supporto non sicuro/adatto, installazione di software non autorizzato sulla postazione di lavoro, divulgazione involontaria delle informazioni (es in un dialogo), attacco di ingegneria sociale per carpire informazioni/furto identità, mancata protezione dei pc (es. schermi non protetti), cambio mansione, dimissioni di dipendente, affidamento di attività di progetto/servizio a fornitori, infezioni da virus/malware, sistema di autenticazione/profilazione/gestione delle credenziali non adeguato, errori/vulnerabilità nel software utilizzato, trasmissioni di dati in maniera non sicura, comportamenti sleali o fraudolenti di dipendenti, furto di dispositivi (pc, telefono, HW). |
| **Integrità – modifica indesiderata dei dati** |
| Installazione di un middleware, software o HW che danneggia i dati, errori in fase di aggiornamento dei S.O., del middleware, delle configurazioni, errori umani involontari di dipendenti (es per poca formazione/competenza, disattenzione, ...), inserimento errato di dati durante la reportistica dei risultati delle analisi o dei controlli, comportamenti sleali o fraudolenti di dipendenti. |
| **Disponibilità – perdita dei dati** |



E-MAIL: dpo@policlinicogemelli.it

| |
|---|
| Infezioni da virus/malware, errori/vulnerabilità nel software utilizzato, errori in fase di aggiornamento dei SO, del middleware, delle configurazioni, errori umani involontari di dipendenti (es per poca formazione/competenza, disattenzione, etc.), evento naturale catastrofico (incendio, inondazione), evento vandalico, furto di dispositivi (pc, telefono, hw), utilizzo di sw contraffatto, dimensionamento non corretto dei repository dei dati (DB, file system), errori in fase di aggiornamento dei sw applicativo, scadenza licenza, mancato aggiornamento middleware, interruzioni o non disponibilità della rete (guasti), indisponibilità del personale (malattia, sciopero, pensionamento, etc.), furto documenti cartacei, guasto hardware, attacchi DOS/DDOS, interruzioni o non disponibilità dei sistemi complementari (elettricità, climatizzazione, etc.). |

### 5.6 Quali sono le fonti di rischio?

| Riservatezza – accesso illegittimo ai dati |
|---|
| Fonti interne umane, fonti esterne non umane. |
| **Integrità – modifica indesiderata dei dati** |
| Fonti interne umane, fonti esterne non umane. |
| **Disponibilità – perdita dei dati** |
| Fonti interne umane, fonti esterne non umane. |

### 5.7 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

| Riservatezza – accesso illegittimo ai dati |
|---|
| Vedi parr 5.1, 5.2, 5.3. |
| **Integrità – modifica indesiderata dei dati** |
| Vedi parr 5.1, 5.2, 5.3. |
| **Disponibilità – perdita dei dati** |
| Vedi parr 5.1, 5.2, 5.3. |

## 6. RISULTATI DPIA E AZIONI DI MIGLIORAMENTO

Dall'analisi sulla gravità e le probabilità dei rischi emerge un valore di **Rischio Inerente** di livello **Moderato.**
Nell'ottica di mitigazione di tali rischi si evince che, con l'implementazione delle misure tecnico/organizzative in atto, **il valore di abbattimento del Rischio Inerente, ovvero il Rischio Residuo, rientra in una condizione di accettabilità da parte dell'organizzazione.**
Al netto delle azioni di miglioramento si ritiene pertanto che **il trattamento in oggetto presenti un grado di rischio accettabile sui diritti e libertà dell'interessato** e di conseguenza non è richiesta una consultazione preventiva all'Autorità Garante.

**N.B Il dettaglio dei valori, dei sistemi di calcolo e delle evidenze che hanno condotto al risultato di accettabilità è presente nella versione integrale della DPIA, a disposizione, su richiesta, del GPDP.**

## 7. RISULTATI DPIA – PARERE DEL DPO

Ai sensi dell'art. 35(2) e art. 39(1) (lett. c) del GDPR, in qualità di Responsabile della protezione dei dati e sulla base di quanto sopra riportato il DPO esprime parere:
favorevole
all'implementazione del trattamento oggetto della presente DPIA.

Firmata digitalmente da

Avv. Francesco Giorgianni

FRANCESCO GIORGIANNI
05/09/2025 15:25:03 UTC+0200

## 8. DOCUMENTI A SUPPORTO

**omissis**



E-MAIL: dpo@policlinicogemelli.it