Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

DATA PROTECTION IMPACT ASSESSMENT
STUDI CLINICI
**ESTRATTO**

ID DELLO STUDIO: 6859

NOME DELLO STUDIO: PITNET

PRINCIPAL INVESTIGATOR: DR. GUIDO RINDI

09/10/2025

## Sommario





E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO



| ATTIVITA' | FUNZIONE | RESPONSABILE | DATA |
|---|---|---|---|
| Redatto da: | Ufficio Privacy | | 09/10/2025 |
| Verificato da: | DPO | Avv. Giorgianni | 09/10/2025 |
| Approvato da: | Direttore Generale | Dr. Daniele Piacentini | 09/10/2025 |


E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

# DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

## 1. CONSIDERAZIONI PRELIMINARI

Questo modello di DPIA è implementato dalla Fondazione Policlinico Gemelli IRCSS per adempiere a quanto previsto dalle indicazioni del GPDP del 6 giugno 2024 "*FAQ - Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca*" a seguito delle modifiche al Codice Privacy introdotte nell'art. 44 comma 1 bis della legge 29 aprile 2024, n. 56.

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".
Inoltre, come riportato nelle FAQ succitate: "***Gli IRCCS possono**, in alternativa* [al consenso, n.d.R], ***fondare il trattamento dei dati personali raccolti per scopi di cura per ulteriori finalità di ricerca in campo medico, biomedico e epidemiologico sull'art. 110-bis**, comma 4 del Codice, in base al quale "Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento".*
*L'art. 110-bis, comma 4 del Codice costituisce una di quelle disposizioni di legge, che si inseriscono nello spazio di normazione lasciato agli Stati membri, ai sensi dell'art. 9, par. 2, lett. j) del Regolamento, alle quali fa riferimento l'art. 110 (primo comma, primo periodo) del Codice nella parte in cui prevede che: "1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, [...] ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento"*."

Nelle medesime FAQ il GPDP specifica gli adempimenti in carico al Titolare che voglia avvalersi del 110 bis:
"*Nel caso in cui gli IRCCS fondino il trattamento dei dati raccolti per finalità di cura per ulteriori finalità di ricerca sull'art. 110-bis, comma 4 del Codice, essi devono obbligatoriamente svolgere e pubblicare la Valutazione d'impatto (VIP) sui propri siti web, in quanto tale articolo costituisce una di quelle disposizioni di legge alle quali fa riferimento l'art. 110 del Codice, prescrivendo tali ulteriori adempimenti*."


E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore



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

### 2.1 SPECIFICARE ID E TITOLO ORIGINALE DELLO STUDIO

Studio PiTNET_2024

ID: 6859

PNRR-TR1-2023-12377961 Studio no-profit co-finanziato da fondi PNRR Next-Generation EU

Titolo: “Valutazione clinico-patologica dei Pit-NETs: dati da un'ampia coorte di pazienti multicentrica.”

Title: “Clinical-pathological assessment of Pit-NETs: data from a large multicenter patients cohort.”

### 2.2 SINOSSI DELLO STUDIO



E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

# DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

| SINOSSI | |
|---|---|
| **TITOLO DELLO STUDIO** | Valutazione clinico-patologica dei Pit-NETs: dati da un'ampia coorte di pazienti multicentrica. |
| **PROMOTORE/SPONSOR** | Fondazione Policlinico Universitario A. Gemelli IRCCS |
| **CRO**<br>***(specificare anche attivita' delegate)*** | Non applicabile |
| **Cofinanziatore**<br>***(specificare se previsto scambio di informazioni di sicurezza)*** | Ministero della Salute<br>Bando PNRR - TR1-2023-12377961 |
| **SPERIMENTATORE PRINCIPALE** | Prof. Guido Rindi |
| **BACKGROUND E RAZIONALE DELLO STUDIO** | Gli adenomi ipofisari, ovvero i tumori neuroendocrini ipofisari (PitNETs), sono riconosciuti come neoplasie rare (codice Orpha 99408) da istituzioni nazionali ed internazionali. Sebbene la maggior parte dei PitNET abbiano una crescita lenta e un comportamento indolente, circa un terzo non raggiunge il controllo biochimico, si ripresenta e ricresce invadendo le strutture circostanti e resistono ai trattamenti convenzionali. Non sono stati identificati predittori di comportamento aggressivo per i PitNET. Nel 2013 Trouillas e colleghi hanno sviluppato un punteggio clinicopatologico a cinque livelli mescolando dati istopatologici e prove clinico-radiologiche di invasione. Questo sistema ha dimostrato di avere valore prognostico. Tuttavia, a differenza dei NET dell'intestino e del polmone, non sono stati sviluppati strumenti formali di classificazione e/o stadiazione dall'OMS nel 2021 e nel 2022. Inoltre, i PitNET non sono stati studiati a fondo dalla radiomica per la previsione del comportamento clinico, né sono stati chiariti pathways farmacologici nelle cellule PitNET per svelare potenzialità per nuovi per approcci terapeutici. Il nostro progetto rappresenta un approccio multidisciplinare di ricerca. Attraverso innovativi studi clinici, di base e modelli traslazionali, il nostro progetto fornirà presto strumenti di valutazione e stadiazione e algoritmi basati sull'apprendimento automatico di identificazione dei PitNET aggressivi con rischio di recidiva/progressione e |





E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

| | |
|---|---|
| | scarsa risposta ai trattamenti convenzionali. Questi nuovi strumenti consentiranno il riconoscimento precoce dei pazienti che necessitano di riferimento a Centri di eccellenza per i tumori ipofisari per sottoporsi a terapie multimodali, personalizzate e mirate, che potenzialmente migliorano l'efficacia nel trattamento dei PitNET aggressivi, il benessere e la qualità della vita dei pazienti, nonché la riduzione dei costi e dell'impatto dei PitNET sulla sistema sanitario nazionale. |
| **OBIETTIVI DELLO STUDIO** | **Primario:**<br><br>definire strumenti di classificazione e stadiazione per PitNETs basati su:<br><br>trascrizione specifica dei fattori (PIT1, T-PIT, SF1);<br><br>specificazione del tipo cellulare mediante produzione di ormoni (prolattina, TSH, LH, FSH, ACTH, GH o nessuno);<br><br>integrazione di misure radiologiche standard con strumenti riconosciuti per la stadiazione clinica e patologica.<br><br>**Secondari:**<br>- indagare le caratteristiche radiomiche/radiologiche come predittori del comportamento, della prognosi, della funzionalità e dell'esito del trattamento dei PitNETs.<br>- indagare se l'espressione di biomarcatori molecolari [Crescita endoteliale vascolare Factor (VEGF), recettore del fattore di crescita epiteliale (EGFR), recettori 1-5 della somatostatina (SSTR), fattore di crescita dei fibroblasti (FGF), mTOR (bersaglio della rapamicina nei mammiferi), Cellule programmate Morte 1 (PD1) e suoi ligandi (PD-L1) e T citotossica associata ai linfociti 4 (CTLA4)] può avere un impatto sulla prognosi dei pazienti |
| **ENDPOINT** | **Primari:** testare la sensibilità e la specificità degli strumenti di classificazione e stadiazione proposti nel predire la recidiva dei PitNETs<br>**Secondari:**<br>- progressione del tumore residuo<br>- resistenza alle terapie convenzionali |

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

| | |
|---|---|
| | - sopravvivenza libera da malattia<br>- sopravvivenza libera da progressione |
| **DISEGNO DELLO STUDIO OGGETTO DELLO STUDIO** | Studio Osservazionale multicentrico ambispettico senza farmaco e senza dispositivo medico |
| **NUMERO DI PAZIENTI presso FPG e totali** | Totali 740 pazienti (540 retrospettivi e 200 prospettici), dei quali retrospettivi 200 e prospettici 100 presso FPG (numero minimo previsto dallo studio) |
| **POPOLAZIONE TARGET** | Pazienti affetti da PitNETs |
| **CRITERI DI INCLUSIONE** | Età >18 anni; disponibilità dei campioni; disponibilità delle immagini radiologiche; follow-up di 5-10 anni. |
| **CRITERI DI ESCLUSIONE** | Minori di 18 anni; indisponibilità dei campioni e delle immagini radiologiche, follow-up minore di 5 anni. |
| **DURATA DELLO STUDIO e DURATA DELL'ARRUOLAMENTO** | Durata dello studio: 24 mesi<br><br>Durata dell'arruolamento: 16 mesi |
| **TRATTAMENTO/PROCEDURA SPERIMENTALE** | 1) Immunoistochimica e proteomica per la valutazione dell'espressione dei recettori della somatostatina, VEGF, EGFR, FGF, PD-1, PD_1L, CTLA-4, mTOR<br>2) Valutazione radiomica delle immaggini neuroradiologiche (MRI)<br>3) Costruzioni e valutazione di modelli prognostici tramite Machine Learning<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. |

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

# DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO



E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

| | |
|---|---|
| **ANALISI STATISTICA e dimensionamento campionario se applicabile** | **Dimensione del campione**<br><br>La dimensione del campione è stata calcolata sulla base dell'obiettivo specifico 1, ipotizzando una frequenza stimata di invasione locale delle strutture circostanti nel 20% dei PitNET trattati chirurgicamente (alfa=0,05; potenza=80%, proporzione complessiva di eventi pari a 0,20). La dimensione del campione ottenuta è N=246 soggetti. Tenendo conto del fatto che gli strumenti di grado e di stadiazione del PitNET saranno costruiti in base ai tre fattori di trascrizione specifici della linea cellulare, 740 casi saranno inclusi nel progetto di ricerca (livello di confidenza 95%, margine di errore: 4,99%), per il braccio retrospettivo dell'obiettivo 1. La coorte di validazione includerà il 20% dei |

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

| | |
|---|---|
| | PitNET trattati chirurgicamente (alfa=0,5; potenza: 0,20). La coorte di validazione includerà 200 pazienti arruolati prospetticamente, in base al numero stimato di pazienti che possono essere inclusi nello studio di periodo da ciascuna unità.<br><br>**Analisi statistica**<br><br>Il campione sarà descritto nelle sue caratteristiche cliniche e demografiche utilizzando tecniche di statistica descrittiva. Le variabili quantitative saranno descritte utilizzando le seguenti misure: minimo, massimo, range, media e deviazione standard. Le variabili qualitative saranno riassunte con tabelle di frequenza assolute e percentuali. La normalità delle variabili continue sarà verificata con il test di Kolmogorov-Smirnov. I pazienti saranno stratificati in base all'esito primario raggiunto (recidiva di PitNETs/non recidiva) e l'analisi statistica sarà eseguita per confrontare i gruppi. I confronti saranno effettuati con test parametrici o non parametrici a seconda della natura dei dati. L'obiettivo specifico1 sarà raggiunto eseguendo una regressione logistica con variabile dipendente la condizione di recidiva/non recidiva di PitNET e variabile indipendente ciascun parametro di patologia e morfologia. Il coefficiente di regressione di ciascuna covariata significativa sarà utilizzato per creare un punteggio assegnando a ciascuna covariata un punteggio che sarà proporzionale al suo coefficiente di regressione. Il punteggio di ogni covariata sarà sommato per calcolare un punteggio cumulativo per ogni paziente, che infine sarà correlato con l'endpoint primario. La sensibilità e la specificità degli strumenti di grado e di stadiazione saranno testate anche su diverse misure di esito, che abbiamo identificato come la progressione del tumore residuo e la resistenza alle terapie convenzionali, la sopravvivenza libera da malattia e la sopravvivenza libera da progressione. In base alla diversa natura degli endpoint (quantitativi continui, politomici o dicotomici) applicheremo diversi algoritmi di apprendimento, tra cui, tra gli altri, Support Vector Machine (SVM), Artificial Neural Networks (ANN), Naïve Bayes (NB), Classification and Regression Trees e metodi ensemble come Random Forest (RF), Gradient Boosting Machine (GBM) e REP-trees. Tutti gli obiettivi secondari saranno |

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

| | |
|---|---|
| | raggiunti con la stessa tecnica. Una serie di tecniche di apprendimento automatico saranno addestrate e testate per estrarre le firme radiomiche più importanti in grado di prevedere il grado e la stadiazione del PitNET, gli esiti della malattia (recidiva, progressione e risposta alle terapie convenzionali, sopravvivenza libera da malattia e sopravvivenza libera da progressione), la consistenza dei tumori e il modello di crescita, estensione e invasione. I modelli ottenuti saranno valutati mediante (i) l'analisi della curva ROC e le relative metriche (esito dicotomico); (ii) l'errore di misclassificazione (esito politomico); (iii) l'errore quadratico medio (esito continuo). I modelli ottenuti saranno confrontati con le prestazioni estratte da modelli parametrici classici (come la regressione logistica per gli esiti binari o la regressione lineare semplice per gli esiti continui). Il metodo di Kaplan-Meier e il test di Log-rank saranno utilizzati per stimare e confrontare due o più curve di sopravvivenza.<br><br>Saranno applicati modelli di regressione a rischi proporzionale di Cox per stimare gli hazard ratio (HR) e gli effetti sulla sopravvivenza dei fattori predittivi per la loro rilevanza prognostica.<br><br>Il valore P < 0,05 è stato considerato statisticamente significativo.<br><br>L'analisi statistica è stata valutata utilizzando il software R, versione 4.4.0 (R Core Team (2024)). |
| **SICUREZZA/GESTIONE EVENTI AVVERSI** | Non Applicabile |
| **DOCUMENTO DI RIFERIMENTO PER LA SICUREZZA** | Non applicabile |
| **BIBLIOGRAFIA** | 1. malattierare.gov.it/malattie/ricerca<br>2. endo-ern.eu/specific-expertise/pituitary/specific-conditions/<br>3. doi:10.1530/EJE-17-0796<br>4. doi:10.1530/EJE-22-0812<br>5. doi:10.3390/cancers12020308<br>6. DOI: 10.1093/neuros/nyab320<br>7. DOI: 10.1001/jamasurg.2020.2713<br>8. doi:10.1038/s41598-017-11104-4<br>9. doi:10.4274/MMJ.galenos.2022.58538 |

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

## 2.3 TIPOLOGIA DI STUDIO

- Multicentrico
- No-profit[1]
- Retrospettivo osservazionale

## 2.4 NUMERO DI PAZIENTI ARRUOLATI

740

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

- **Riportare una riga di dataset (es. CRF)**

  Vedi allegato Power Point della CRF

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

  I dati raccolti dai partecipanti agli studi sono pseudoanomizzati attraverso l'utilizzo di un ID univoco generato automaticamente da RECap e dal codice interno ospedaliero. Per FPG il codice sanitario è un codice che consente l'identificazione del paziente solo tramite accesso ai sistemi interni della fondazione (Trackare) accesso che avviene tramite autenticazione con matricola e pw e previa abilitazione all'accesso da parte di ICT. Al di fuori dell'ospedale il codice non consente di risalire al paziente nemmeno attraverso l'incrocio di altri dati.

- **La tabella di conversione è conservata in un luogo/software separato rispetto al dato pseudonimizzato? (specificare la modalità)**

[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

Si, la tabella di conversione è conservata separatamente rispetto al dato pseudonimizzato, in quanto il dato clinico raccolto si trova sul server dove è istallato REDCap* mentre la tabella di conversione è conservata attraverso i sistemi informativi di ciascun centro partecipante.

* Per i server REDCap: Gli ambienti di storage sono tutti GDPR compliant:
  - Databases criptati sotto dominio FPG
  - Isolamento VLAN: Front end e back end di REDCap giacciono su subnet distinte:
    - Frontend: PHP Apache su Red Hat Enterprise Linux 8 su subnet dedicate.
    - Backend: MySQL su Red Hat Enterprise Linux 8 su subnet dedicate.
  - Protezione dati in transit: TLS 1.3

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

Implementazione di salti logici tra domande e/o sezioni per guidare la compilazione e campi calcolati per limitare errori di inserimento evitabili con una configurazione di sistema
Implementazione by design di sistemi di validazione sintattica e semantica delle variabili principali:

- Limitazioni alla tipologia di dato che può essere inserito
- Range di validità dei dati inseriti (alert o bloccanti)
- Mandatorietà (inclusa gestione dei Missing data)
- Etichettatura di dati sensibili (per limitarne l'export) (a riguardo a breve verrà approvata da FPG una procedura operativa standard Estrazione/Importazione dati in studi clinici no profit)
- Compilazione di determinate variabili solo coerentemente rispetto a step precedenti di compilazione
- Aggiunta di note utili alla compilazione.

Impostazioni di regole di data quality per il controllo in background o a posteriori dei dati inseriti attraverso il pannello "Data quality".
Configurazione funzionalità Data Resolution Workflow (Data Queries); per abilitare un workflow di gestione di correzioni da apportare ai dati
Funzionalità utili per l'audit trail (History, logging ecc).

- **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, mediante incontri a cadenza mensile che coinvolgono tutto il gruppo di studio.

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore



## 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

- 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 | RedCap | eCRF | | |
| 2 | R e Stata 17 | Data cleaning, processing e analisi | | |
| 3 | 3D Slicer | Visualizzazione e contornazione MRI | | |
| 4 | ITK-Snap | Visualizzazione e contornazione MRI | | |
| 5 | RStudio con linguaggio di programmazione R | Programmare e fare analisi dati/immagini e modellistica | | |
| 6 | Visual Studio Code | Programmare e fare analisi dati/immagini e modellistica | | |
| 7 | Python | Programmare e fare analisi dati/immagini e modellistica | | |



E-MAIL: dpo@policlinicogemelli.it

## 2.7 CRF/ECRF

- **In caso di eCRF indicare software/piattaforma utilizzata**

Redcap Research Electronic Data Capture

- **Indicare se il software/ piattaforma utilizzata è di proprietà di Fondazione o di un fornitore esterno (outsourcing)**

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

- **In caso di outsourcing indicare fornitore della piattaforma**

N/A

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

È previsto lo scambio di file, in particolare di immagini MRI tra i centri satellite e FPG. Il trasferimento delle immagini MRI dagli altri centri avverrà tramite link a cartelle condivise sul OneDrive istituzionale dell'account della Facility GSTeP di Radiomica (@radiomics.gstep). I referenti di ogni centro avranno accesso solamente alla cartella relativa al proprio centro tramite autenticazione a 2 fattori.

- **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.



E-MAIL: dpo@policlinicogemelli.it

## 2.8 CAMPIONI BIOLOGICI

N\A

## 2.9 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

## 2.10 RUOLI PRIVACY

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

- **Eventuali autonomi titolari – Centri Partecipanti** ☒ SI ☐ NO

| | Autonomi titolari | Indirizzo |
|---|---|---|
| 1 | Azienda ospedaliera universitaria Federico II | Via Sergio Pansini, 5, 80131 Napoli NA |
| 2 | IRCCS Ospedale San Raffaele | |
| 3 | Azienda Ospedaliera Universitaria Gaetano Martino | Via Consolare Valeria, 1, 98124 Messina ME |


E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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

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

| | Nome Fornitore | Indirizzo |
|---|---|---|
| 1 | \ | |

  - 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 | \ | | |

  - Contract Research Organization (CRO) ☐ SI ☒ NO

Se sì, specificare Nome, indirizzo e PEC della CRO

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

| | Nome laboratorio | Indirizzo | Ruolo Privacy |
|---|---|---|---|
| 1 | \ | | |

## 2.1 Trasferimenti dati extra UE

I dati sono trasferiti extra UE

☐ SI ☒ NO



E-MAIL: dpo@policlinicogemelli.it

I dati dei pazienti FPG non vengono trasferiti presso il Centro partecipante.

## 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 | | | |

#### 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 |
|---|---|---|---|---|
| | 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

### 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 e come meglio specificato nelle FAQ (*Presupposti giuridici e principali adempimenti per il*

*trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca*) pubblicate dal GPDP e di seguito riportate:

"*Gli IRCCS possono, in alternativa* [al consenso n.d.R]*, fondare il trattamento dei dati personali raccolti per scopi di cura per ulteriori finalità di ricerca in campo medico, biomedico e epidemiologico sull'art. 110-bis, comma 4 del Codice, in base al quale "Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento*".

| 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 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:



E-MAIL: dpo@policlinicogemelli.it

- 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.
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)


E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore



**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, ad ex: 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.<br>• 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 software/ Piattaforma fanno parte del Portafoglio Applicativo FPG |
| 3 | La tabella di conversione è conservata in un luogo/software separato rispetto al dato pseudonimizzato |



E-MAIL: dpo@policlinicogemelli.it

| | |
|---|---|
| 4 | I codici pseudonimizzati rispettano la previsione di non inserire riferimenti identificativi dei pazienti |
| 5 | Il trattamento dei dati personali avviene solo tramite dispositivi/ personal computer aziendali |
| 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 | Il file contenente le ecrf è cifrato e conservato su dispositivi FPG |
| 11 | La piattaforma ECRF è in https |
| 12 | Se ai fini dello Studio verranno usati o testati o sviluppati algoritmi di IA si attesta che:<br>a) c'è una valutazione del codice utilizzato (ad esempio per vagliare la presenza di backdoor)<br>b) tutti i processi automatizzati sono sotto controllo umano. |

## 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; i responsabili ex art 28 hanno apposito atto di nomina; eventuali trasferimenti extra UE sono regolati attraverso appositi strumenti come SCC, DTA (data transfer agreement), decisioni di adeguatezza, DPF (data privacy framework). |
| 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. |

| | | |
|---|---|---|
| | | 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 |

## 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: |


E-MAIL: dpo@policlinicogemelli.it

- 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 |
| 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. |



E-MAIL: dpo@policlinicogemelli.it

| 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** (in una scala che prevede valori da lieve a moderato a grave a molto grave)

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.


E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore



Firmata digitalmente da

Avv. Francesco Giorgianni

## 8. DOCUMENTI A SUPPORTO

**omissis**



E-MAIL: dpo@policlinicogemelli.it