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: 6868

NOME DELLO STUDIO: ROAR

PRINCIPAL INVESTIGATOR: PROF.SSA MARIA GABRIELLA FERRANDINA

16/09/2025

Sommario

E-MAIL: dpo@policlinicogemelli.it

ATTIVITA'	FUNZIONE	RESPONSABILE	DATA
Redatto da:	Ufficio Privacy		15/09/2025
Verificato da:	DPO	Avv. Giorgianni	15/09/2025
Approvato da:	Direttore Generale	Dr. Daniele Piacentini	15/09/2025

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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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

2.1 SPECIFICARE ID E TITOLO ORIGINALE DELLO STUDIO

ID: 6868 – STUDIO ROAR

Studio no-profit co-finanziato dal Ministero della Salute con fondi PNRR Next-Generation EU PNRR: PNRR-TR1-2023-12378400

Titolo: UNDERSTANDING THE RAREST GYNECOLOGICAL CANCERS: A MULTI -OMICS PLATFORM FOR IMPROVED PATIENTS' MANAGEMENT

2.2 SINOSSI DELLO STUDIO

SINOSSI	
TITOLO DELLO STUDIO	COMPRENSIONE DEI TUMORI GINECOLOGICI PIÙ RARI: UNA PIATTAFORMA MULTI-OMICA PER UNA MIGLIORE GESTIONE DEI PAZIENTI
PROMOTORE/SPONSOR	Fondazione Policlinico Universitario A. Gemelli IRCCS
CRO *(specificare anche attivita' delegate)*	Non applicabile
Cofinanziatore ***(specificare se previsto scambio di informazioni di sicurezza)***	MINISTERO DELLA SALUTE PNRR: PNRR-TR1-2023-12378400
SPERIMENTATORE PRINCIPALE	Prof.ssa Maria Gabriella Ferrandina
BACKGROUND E RAZIONALE DELLO STUDIO	I tumori ginecologici rari, tra cui i sarcomi uterini, i tumori vulvari e i tumori ovarici non epiteliali, sono malattie poco studiate e l'assenza di approcci diagnostici e terapeutici standardizzati o di linee guida cliniche personalizzate ha portato a bassi tassi di

E-MAIL: dpo@policlinicogemelli.it

	sopravvivenza e/o a scarsa qualità della vita. Il progetto ROAR mira ad aumentare la comprensione molecolare di queste malattie in un contesto multidisciplinare e interistituzionale che comprende ginecologi oncologi, oncologi medici, ricercatori di fase I, patologi, patologi molecolari, infermieri di ricerca, genetisti, bioinformatici, psicologi e gruppi di pazienti
OBIETTIVI DELLO STUDIO	**Primario:** 1. Rivedere i dati disponibili sui RGC, implementare procedure di cura standard per i RGC in tutti i centri coinvolti e creare l'infrastruttura per gestire il progetto. Questo obiettivo rientra nei seguenti pacchetti di lavoro (WP). 2. Integrazione e implementazione dell'archiviazione di campioni annotati di alta qualità, della raccolta di dati clinici e della generazione di dati molecolari multi-omici in una banca dati dedicata alle RGC. 3. Impatto dei dati molecolari sulla gestione clinica delle pazienti affette da tumori ginecologici rari. **Secondari:** Armonizzazione delle linee guida o delle raccomandazioni. Questo compito consiste nell'integrare tutti i dati del progetto ROAR per aggiornare le linee guida cliniche o fornire nuove raccomandazioni per ogni tumore ginecologico raro incluso.
ENDPOINT	**Primari:** 1. Armonizzare le procedure e consentire una facile e sicura condivisione dei dati tra tutte le istituzioni coinvolte 2. Esecuzione di una profilazione somatica e trascrizionale completa e una valutazione del profilo immunologico su campioni di alta qualità conservati in una biobanca dedicata ai tumori ginecologici rari; **Secondari:** Valutare l'impatto clinico del comitato sulla gestione dei tumori ginecologici rari e, attraverso le evidenze raccolte, implementare strategie diagnostiche e terapeutiche
DISEGNO DELLO STUDIO OGGETTO DELLO STUDIO	Studio osservazionale multicentrico, ambispettico senza farmaco e senza dispositivo medico

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

NUMERO DI Pazienti presso FPG e totali	190 pazienti tra il centro Promotore e i centri partecipanti
POPOLAZIONE TARGET	30 pazienti con tumori ovarici non epiteliali, 40 sarcomi uterini e 120 tumori vulvari.
CRITERI DI INCLUSIONE	>18 anni Diagnosi istologica di: - tumori ovarici non epiteliali - sarcomi uterini - tumori vulvari.
CRITERI DI ESCLUSIONE	Infezione da HIV, HBV o HCV attive Neoplasie sincrone Istologie non rare
PIANO STATISTICO	La sfida di questo studio è quella di indagare l'eventuale presenza di alterazioni che possono essere possibili target farmacologici in questi gruppi di tumori rari e con poche possibilità terapeutiche. In questo progetto non sono previsti test di ipotesi formali, sia per l'intento esplorativo che per la rarità di questi tipi di tumori. Anche i vincoli economici rappresentano un limite per molti degli approcci proposti. In base a una fattibilità pre-studio nei centri partecipanti, si presume di poter includere in questa ricerca circa 30 tumori ovarici non epiteliali, 40 sarcomi uterini e 120 tumori vulvari. Per ogni paziente saranno raccolti contemporaneamente diversi campioni di sangue, di tessuto neoplastico e di tessuto sano anche durante il follow-up per ripetere i prelievi di sangue. Le analisi si articoleranno su più livelli. Innanzitutto, verrà utilizzato un approccio descrittivo. Le caratteristiche demografiche e cliniche e i dati molecolari saranno riassunti per tipo di tumore utilizzando conteggi assoluti e percentuali se riferiti a elementi categorici o calcolando media e deviazioni standard nonché mediana, intervallo interquartile, minimo e massimo per le variabili quantitative. Si procederà quindi a un'analisi esplorativa dei dati cercando di rispondere, attraverso la visualizzazione, la trasformazione e la

E-MAIL: dpo@policlinicogemelli.it

	modellizzazione, a domande sui dati come gli outlier, le correlazioni tra le variabili, la stima della variabilità. L'approccio comparativo a questi dati partirà dalla riduzione del numero di variabili considerate. I dati appaiati sugli stessi pazienti saranno confrontati con il test t di Student e sarà adottata una procedura Benjamini-Hochberg per identificare i fattori che differenziano i due tipi di tessuto (neoplastico e sano) tenendo sotto controllo il False Discovery Rate. Una volta ridotto il numero di variabili candidate, verranno implementati modelli misti per comprendere le differenze tra campioni di tessuti di natura diversa provenienti dagli stessi pazienti. Quando si analizza il profilo molecolare in base al tipo di tumore, come primo passo si cercherà di ridurre la dimensionalità calcolando la correlazione tra le variabili per evitare la multicollinearità. Su elementi selezionati implementeremo un'analisi di cluster non supervisionata per comprendere le strutture sottostanti ai dati. Le tecniche di clustering (ad esempio, clustering gerarchico, clustering k-means) e i metodi di riduzione della dimensionalità (ad esempio, analisi delle componenti principali) saranno utilizzati per raggruppare campioni simili o identificare modelli nei dati. I fattori strutturali saranno poi impiegati nella costruzione di algoritmi di classificazione come le macchine a vettori di supporto (SVM), le foreste casuali o le reti neurali per prevedere gli esiti della malattia sulla base delle caratteristiche genomiche. L'analisi dei dati della biopsia liquida consisterà principalmente nel rilevare l'anticipazione della malattia progressiva rispetto alle procedure diagnostiche standard. La concordanza dei due metodi (positività del ctDNA e progressione valutata secondo RECIST 1.1) e il tempo di latenza tra di essi saranno ampiamente descritti. La concordanza sarà valutata utilizzando la statistica kappa e le eventuali differenze nel tempo alla progressione saranno valutate con il test di Wilcoxon signed-rank. A causa dello stato esplorativo di questo progetto e dei problemi di molteplicità, i risultati saranno di natura ipotetica e dovranno essere convalidati in serie esterne.

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DURATA DELLO STUDIO e DURATA DELL'ARRUOLAMENTO	24 mesi
TRATTAMENTO/PROCEDURA SPERIMENTALE	N/A
ANALISI STATISTICA e dimensionamento campionario se applicabile	Secondo uno studio di fattibilità preliminare condotto tra i centri partecipanti, prevediamo di poter includere circa 30 tumori ovarici non epiteliali, 40 sarcomi uterini e 120 tumori vulvari in questa ricerca.
SICUREZZA/GESTIONE EVENTI AVVERSI	Tutti gli eventi osservati durante lo studio verranno raccolti e registrati secondo le normative vigenti. 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	Non applicabile

2.3 TIPOLOGIA DI STUDIO

- Multicentrico
- No-profit co-finanziato1
- Retrospettivo osservazionale (ambispettico: DPIA svolta per la sola corte retrospettiva)

2.4 NUMERO DI PAZIENTI ARRUOLATI

190 pazienti tra il centro Promotore e i centri partecipanti di cui, per la coorte retrospettiva: 52 pazienti presso il centro Promotore

[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

2.5 DATASET, PSEUDONIMIZZAZIONE, CONTROLLI DI INTEGRITÀ, DATA BREACH

- Riportare una riga di dataset (es. CRF)

Vedi allegato relativo alla eCRF ENDOCancer-data

- 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.
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;

E-MAIL: dpo@policlinicogemelli.it

- 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 pseudonimizzato? (specificare la modalità)

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)

Lo scenario di data breach è stato affrontato dal PI durante la riunione di presentazione dello studio, tenutasi in data 20 settembre 2024. In tale occasione, il PI ha illustrato le procedure da seguire in caso di data breach, sottolineando l'importanza della tempestiva segnalazione dell'evento al Responsabile della Protezione dei Dati (DPO) e all'Autorità Competente, in conformità al Regolamento (UE) 2016/679 (GDPR) e alle policy interne dell'ente.
La comunicazione è avvenuta in forma orale, durante la riunione sopra citata, alla presenza del personale coinvolto nello studio.
Il PI ha inoltre previsto che tali aspetti relativi alla gestione di eventuali data breach verranno richiamati e approfonditi anche nel corso delle prossime riunioni di aggiornamento dello studio, al fine di garantirne la costante condivisione e il rafforzamento della consapevolezza tra tutti i soggetti coinvolti.

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)	Raccolta, gestione, interrogazione dati clinici (eCRF)	Installato in FPG	Vanderbilt University / Open source
2	cBioPortal	Interrogazione dati, estrazione dati, analisi dati	Installato in FPG	Open source
3	SlideViewer	software per la visualizzazione dei vetrini digitalizzati. Si tratta di un software proprietario dell'azienda che fornisce lo scanner utilizzato per digitalizzare i vetrini di patologia	Installato in FPG	3DHISTECH
4	R	Software di analisi statistica	Installato in FPG	Open source
5	STATA	Software di analisi statistica	Installato in FPG	
6	NCSS	Software di analisi statistica per il calcolo del sample size	Installato in FPG	

NB: I software STATA e NCSS sono installati on premises con regolare licenza d'uso ma non sono oggetto di contratti di manutenzione: i dati personali trattati con questi software non sono dunque nelle disponibilità dei fornitori, che non rivestono dunque il ruolo di responsabili del trattamento.

2.7 CRF/ECRF

- In caso di eCRF indicare software/piattaforma utilizzata

REDCap

E-MAIL: dpo@policlinicogemelli.it

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)

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 CAMPIONI BIOLOGICI

Ogni centro prevede uno stoccaggio autonomo, la Fondazione conserva i campioni nella propria Biobanca.

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

- Azienda Ospedaliera per l'emergenza Cannizzaro
- Istituto Nazionale Tumori "Fondazione Pascale" IRCCS

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

E-MAIL: dpo@policlinicogemelli.it

☐ 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			

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: • Misure di pseudonimizzazione e crittografia dei dati personali • 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 • 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 • 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 • 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 • Misure per la protezione dei dati durante la trasmissione: ex VPN, Autenticazione a più fattori • Misure per la protezione dei dati durante l'archiviazione: ex Crittografia, Backup • 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. • 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; • 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	L' integrità del dato è garantita da log di accesso e modifica e da periodiche revisioni di tali log
6	Il trattamento dei dati personali avviene solo tramite dispositivi/ personal computer aziendali
7	l'accesso al software/piattaforma/piattaforma ECRF contenente i dati avverrà con credenziali personali
8	La piattaforma ECRF è raggiungibile via protocollo https
9	Il file contenente le ecrf è cifrato e conservato su dispositivi FPG

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. Sono, inoltre, previsti degli specifici eventi formativi, in relazione agli specifici settori di competenza. 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: • Perdita di riservatezza dei dati personali protetti da segreto professionale; • Conoscenza da parte di terzi non autorizzati di dati particolari laddove si riesca a re-identificare l'interessato; • 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: • Perdita del controllo della qualità del dato. • 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: • 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.
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.**

E-MAIL: dpo@policlinicogemelli.it

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
17/09/2025 18:39:49 UTC+0200

8. DOCUMENTI A SUPPORTO

omissis

E-MAIL: dpo@policlinicogemelli.it