Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT STUDI CLINICI EX ART. 110 BIS - ESTRATTO

DATA PROTECTION IMPACT ASSESSMENT
ESTRATTO

ID DELLO STUDIO: B3D

PRINCIPAL INVESTIGATOR: DR.SSA LUCIA RICCI-VITIANI

18/06/2025

Sommario

E-MAIL: dpo@policlinicogemelli.it

E-MAIL: dpo@policlinicogemelli.it

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT STUDI CLINICI EX ART. 110 BIS - ESTRATTO

1. CONSIDERAZIONI PRELIMINARI

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

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

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

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

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

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

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

- la presente DPIA è stata elaborata su specifica richiesta del Promotore dello Studio ed ha, pertanto, riguardo solo ed esclusivamente in merito alle attività di pertinenza della Fondazione relative allo sviluppo di un algoritmo basato sull'intelligenza artificiale (AI) in grado di prevedere la sensibilità delle linee GSC a un pannello di farmaci approvati dall'EMA sulla base di dati omici e clinici e di confrontare

E-MAIL: dpo@policlinicogemelli.it

tale sensibilità prevista con la sensibilità effettiva delle GSC in vitro; la Fondazione declina ogni responsabilità per tutti quanti gli aspetti dello Studio in oggetto che non ricadano sotto la diretta supervisione della Fondazione stessa.

- Il presente documento è la versione in estratto della DPIA originale, da cui sono stati rimossi tutti gli elementi potenzialmente lesivi della postura cyber della Fondazione, come da **Ricerca scientifica: le Faq del Garante Privacy per gli IRCCS.**

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

2.1 Specificare ID e Titolo originale dello Studio

B3D - Biobanking, data Biomarkers and Big for personalized treatment of glioblastoma

2.2 Sinossi dello Studio (come da Protocollo)

E-MAIL: dpo@policlinicogemelli.it

DATA PROTECTION IMPACT ASSESSMENT STUDI CLINICI EX ART. 110 BIS - ESTRATTO

I Gliomi di alto grado, incluso glioblastoma (GBM), sono tumori cerebrali rari e altamente aggressivi con una prognosi infausta (sopravvivenza globale mediana 15 mesi). Le caratteristiche aggressive dei gliomi di alto grado, in particolare il GBM, come l'alta frequenza di recidiva e la resistenza alla terapia, sono attribuite a una piccola frazione di cellule con caratteristiche simili a quelle delle cellule staminali, note come cellule staminali di glioblastoma (GSC), che si localizzano preferibilmente nelle nicchie perivascolari. Abbiamo isolato e convalidato GSC da diversi pazienti. La scoperta che il GBM contiene cellule staminali tumorigeniche offre nuove opzioni per terapie mirate al compartimento delle cellule staminali. Lo studio si propone di:
i) impostare un flusso di lavoro stabile per la generazione e l'archiviazione di GSC derivate dal paziente;
ii) eseguire una caratterizzazione completa e multi-omica delle GSC;
iii) verificare la presenza di marcatori in grado di prevedere la sensibilità delle linee GSC a un pannello di farmaci approvati dall'EMA sulla base di dati omici e clinici e di confrontare tale sensibilità prevista con la sensibilità effettiva delle GSC in vitro.
I primi 2 obiettivi e parte del terzo obiettivo del progetto PNRR-TR1-2023-12377972 sono già stati oggetto di valutazione da parte del Comitato Etico Nazionale che in data 26/07/2024 ha espresso parere favorevole al protocollo dal titolo: "Biobanking and Biomarkers for personalized treatment of glioblastoma".
Il presente emendamento si propone di generare un algoritmo basato sull'intelligenza artificiale (AI) in grado di prevedere la sensibilità delle linee GSC a un pannello di farmaci approvati dall'EMA sulla base di dati omici e clinici e di confrontare tale sensibilità prevista con la sensibilità effettiva delle GSC in vitro.

2.3 Tipologia Di Studio

- Multicentrico
- No-profit co-finanziato[1]

2.4 Numero Di Pazienti Arruolati

80

2.5 Database E Software Utilizzati

- I database aziendali utilizzati per raccogliere i dati da utilizzare per lo Studio: TrakCare, Digistat, PACS, Armonia.

E-MAIL: dpo@policlinicogemelli.it

DATA PROTECTION IMPACT ASSESSMENT STUDI CLINICI EX ART. 110 BIS - ESTRATTO

- Per lo studio è necessario inoltre 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	CCLE	Caratterizzazione molecolare; Libreria da cui si scaricano informazioni utili per processare i dati; **nessun dato personale viene trattato tramite questo software**.	cloud	Open source
2	CTRP Libreria da cui si scaricano info utili per processare i dati	Sensitività di linee cellulari; Libreria da cui si scaricano informazioni utili per processare i dati; **nessun dato personale viene trattato tramite questo software**	cloud	Open source
3	Project Achilles Libreria da cui si scaricano info utili per processare i dati	Sensitività di linee cellulari; Libreria da cui si scaricano informazioni utili per processare i dati; **nessun dato personale viene trattato tramite questo software**	cloud	Open source
4	Tensorflow/pytorch/scikitlearn	Librerie machine learning; Software per machine learning	Installati presso il data center FPG	Open source

E-MAIL: dpo@policlinicogemelli.it

5	RedCap	Software per ecrf	Installato presso il data center FPG	software gratuito per la raccolta e la gestione dati, sviluppato e fornito da Vanderbilt University.
6	GARR filesender	Servizio per invio di files di grandi dimensioni	In cloud presso Consortium Garr	Servizio compreso nell'accordo di adesione al Consorzio Garr per collegamento rete dati

2.6 CRF/eCRF e trasferimento files

- software/piattaforma utilizzata:
  RedCap: (in gestione alla facility FPG "Data Collection": i dati ivi presenti vengono estratti e consegnati alla facility di bioinformatica e concorrono alle analisi di machine learning)
- La modalità di trasferimento di files dipende dalla loro grandezza. Generalmente viene utilizzata una cartella condivisa dello SharePoint della Fondazione Gemelli ma, nel caso file piu grandi (superiore ad 1 Gb), la modalità di trasferimento sarà GARR filesender con md5 checksum.

2.7 Risorse: Soggetti interni coinvolti nello studio (ruoli e funzioni)

Tutti i soggetti che tratteranno i dati personali all'interno della Fondazione sono stati nominati soggetti incaricati del trattamento come da Istruzione Operativa - IO.018.

2.8 Ruoli Privacy

- **Titolare del Trattamento** (Promotore): ISS – Istituto Superiore di Sanità

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

- **Responsabili del trattamento** ex art. 28 GDPR
  Fondazione Policlinico Gemelli nel ruolo di Centro di Sperimentazione

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

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

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

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

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

  - Contract Research Organization (CRO) ☐ SI ☒ NO

  - Ulteriori eventuali responsabili del trattamento ☐ SI ☒ NO

E-MAIL: dpo@policlinicogemelli.it

2.9 Trasferimenti dati extra UE

I dati sono trasferiti extra UE

☐ SI ☒ NO

3. PRINCIPI FONDAMENTALI

3.1 Proporzionalità e necessità

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

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

E-MAIL: dpo@policlinicogemelli.it

- 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;
- 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;

E-MAIL: dpo@policlinicogemelli.it

- 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. Inoltre il corretto trasferimento

dei dati da ISS a Fondazione Policlinico verrà controllato tramite md5 checksum; i files una volta pervenuti sono processati attraverso sistemi in grado di generare log riportanti i timestamp delle eventuali modifiche ad essi apportate.

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 in estratto sul sito aziendale nella sezione del sito:

https://www.policlinicogemelli.it/servizi-paziente/privacy-e-protezione-dei-dati-personali/

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

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

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.

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

E-MAIL: dpo@policlinicogemelli.it

4. CALCOLO DEL RISCHIO

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

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

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

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

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

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

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

E-MAIL: dpo@policlinicogemelli.it

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

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

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

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

5. ANALISI DEI RISCHI

5.1 Tabella delle Contromisure tecniche

ID	Misure
1	I dati dello studio sono trattati tramite software installati su sistemi FPG e di conseguenza protetti dai sistemi e dalle policies di cybersecurity di FPG, che comprendono: • 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: 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

E-MAIL: dpo@policlinicogemelli.it

	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 dati dello studio sono caricati in cloud gestiti da Fornitori FPG iscritti nell'albo fornitori e provvisti di regolare contratto e atto di nomina a responsabile del trattamento
3	I software/ Piattaforma fanno parte del Portafoglio Applicativo FPG
4	La tabella di conversione è conservata in un luogo/software separato rispetto al dato pseudonimizzato
5	I codici pseudonimizzati rispettano la previsione di non inserire riferimenti identificativi dei pazienti
6	I dati eventualmente trasmessi all' esterno sono inviati tramite canali protetti/cifrati
7	L' integrità del dato è garantita da log di accesso e modifica e da periodiche revisioni di tali log
8	Il trattamento dei dati personali avviene solo tramite dispositivi/ personal computer aziendali
9	l'accesso al software/piattaforma/piattaforma ECRF contenente i dati avverrà con credenziali personali
10	La piattaforma ECRF è raggiungibile via protocollo https
11	Il file contenente le ecrf è cifrato e conservato su dispositivi FPG
12	I files contenuti nei supporti fisici sono cifrati
13	Se ai fini dello Studio verranno usati o testati o sviluppati algoritmi di IA si attesta che: a) c'è una valutazione del codice utilizzato (ad esempio per vagliare la presenza di backdoor) b) tutti i processi automatizzati sono sotto controllo umano: nel ciclo di vita del modello di intelligenza artificiale utilizzato per l'analisi sono previsti meccanismi strutturati di controllo umano (Human Oversight) volti a garantire la correttezza, l'affidabilità e la conformità etico-legale del sistema. In particolare: • Gli esperti clinici e bioinformatici partecipano attivamente alla definizione del problema, alla selezione delle variabili rilevanti e all'interpretazione dei risultati. • I dati utilizzati sono sottoposti a validazione e controllo di qualità manuale, con attenzione a errori sistematici e bias. • Il modello è testato con supervisione umana in fase di validazione e in scenari simulati, al fine di verificare le prestazioni reali e la coerenza clinica delle predizioni. • Sono adottati strumenti di spiegabilità del modello (es. SHAP) per consentire agli operatori di comprendere le decisioni dell'AI. • È previsto un monitoraggio continuo post-deployment, con la possibilità di intervento umano in caso di anomalie, degrado delle prestazioni o impatti inattesi.

5.2 Tabella delle Contromisure logistiche

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

5.3 Tabella delle Contromisure Organizzative

ID	Misure	Evidenze
1	Ruoli e responsabilità	Descritte nella IO 0.18 per i soggetti interni e descritte per lo studio in oggetto nei parr.2.7 e 2.8. Per tutti i responsabili ex art. 28 GDPR sono predisposti atti di nomina.
2	Formazione	Il Titolare attua una specifica attività di formazione per il personale e per i soggetti coinvolti nella gestione del trattamento dei dati personali, al fine di presidiare adeguatamente le istruzioni fornite e, in ogni caso, di promuovere la cultura della privacy e della sicurezza delle persone fisiche con riguardo ai dati personali all'interno dell'organizzazione aziendale. 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

E-MAIL: dpo@policlinicogemelli.it

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

E-MAIL: dpo@policlinicogemelli.it

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.

E-MAIL: dpo@policlinicogemelli.it

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

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

6. RISULTATI DPIA E AZIONI DI MIGLIORAMENTO

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

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

7. RISULTATI DPIA – PARERE DEL DPO

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

Data Firma

E-MAIL: dpo@policlinicogemelli.it

18/06/2025

Avv. Francesco Giorgianni

GIORGIANNI FRANCESCO
23/06/2025 13:19:30 UTC+0200

8. DOCUMENTI A SUPPORTO

omissis