Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI

DATA PROTECTION IMPACT ASSESSMENT
ESTRATTO

ID DELLO STUDIO: 4224

PRINCIPAL INVESTIGATOR: PROF.SSA ANNA FAGOTTI

15/09/2025

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

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI

1. CONSIDERAZIONI PRELIMINARI

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

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

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

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

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

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

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

E-MAIL: dpo@policlinicogemelli.it

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

2.1 SPECIFICARE ID E TITOLO ORIGINALE DELLO STUDIO

La piattaforma delle portatrici di mutazioni nei geni BRCA: uno studio multicentrico – ID 4224

2.2 SINOSSI DELLO STUDIO

Background: I soggetti portatori di mutazioni nei geni BRCA1 e BRCA2 hanno un maggior rischio di sviluppare diversi tipi di tumori. Nonostante le innumerevoli evidenze scientifiche pubblicate in letteratura negli ultimi due decenni, la gestione di questi soggetti non è ancora completamente definita (1,2). Poiché si stima che la prevalenza delle mutazioni patogenetiche nei geni BRCA è di circa 1:400 - 1:500 individui (3), il numero totale dei portatori è di circa 140.000 - 150.000, nella popolazione italiana. Si stima che l'87% delle donne con mutazioni BRCA andranno incontro, nel corso della loro vita, ad un tumore di origine genetica. Circa il 20% dei 5200 casi di cancro ovarico, diagnosticati ogni anno in Italia, ha un'origine genetica e potrebbe potenzialmente essere oggetto di prevenzione primaria. Attualmente non è ancora stata istituita una raccolta dati prospettica nazionale sulle donne con mutazioni BRCA.
Razionale: Il National Comprehensive Cancer Network (NCCN) ha recentemente pubblicato le linee guida per la gestione degli individui con alto rischio genetico/familiare per il cancro alla mammella e alle ovaie, evidenziando come molti punti debbano ancora essere chiariti a causa della scarsità di dati presenti in letteratura su questa popolazione di donne (4). Questo è il motivo per cui proponiamo la creazione di una piattaforma in cui vengano registrati i dati riguardanti le portatrici di mutazioni patogenetiche nei geni BRCA. La piattaforma è un sistema organizzato che utilizza metodi osservazionali per raccogliere dati uniformi su una popolazione definita da una particolare malattia e che viene seguita nel tempo.
Tipo di studio e durata: Studio osservazionale multicentrico ambispettico Studio retrospettivo osservazionale: da gennaio 2010 Durata dello studio prospettico osservazionale: 240 mesi
Outcome primario: Raccogliere i dati di ogni donna portatrice di mutazioni patogenetiche nei geni BRCA 1/2.
Outcomes secondari: 1. distribuzione geografica delle mutazioni brca e definizione delle mutazioni foundere 2. Identificazione delle aree in cui l'incidenza della mutazione è più alta del previsto 3. centralizzazione dei casi in centri altamente specializzati per la prevenzione e il trattamento del cancro relato alla genetica 4. definizione della relazione tra mutazioni specifiche e l'insorgenza di specifici tipi di cancro 5. valutazione dell'adeguatezza dei criteri per determinare l'accesso alla valutazione genetica

E-MAIL: dpo@policlinicogemelli.it

6. analizzare fattori di rischio dello stile di vita per lo sviluppo di tumori nei portatori di mutazioni brca 7. soggetti sani: analizzare le strategie di riduzione del rischio o di prevenzione 1. il ruolo della chemioprevenzione 2. il ruolo della sorveglianza 3. analizzare l'impatto della salpingo-ovariectomia nella riduzione del rischio di cancro al seno pag. 3 4. analizzare l'impatto della mastectomia profilattica nella riduzione dell'incidenza del cancro al seno 8. valutazione delle donne dopo l'annessiectomia profiliattico a. qualità della vita dopo l'intervento b. funzione sessuale dopo l'intervento c. salute delle ossa dopo l'intervento d. salute cardiovascolare dopo l'intervento e. fertilità dopo l'intervento chirurgico f. alternative di hrt dopo la chirurgia g. esito dei pazienti con cancro al seno 10. follow delle pazienti con cancro alle ovaie.
Piano Statistico (dimensionamento del campione ed analisi dei dati): Data la natura retrospettiva dello studio e l'obiettivo primario puramente descrittivo, proponiamo una dimensione del campione di N= 6500 pazienti per la parte retrospettiva dello studio. Mentre per la parte prospettica dello studio è previsto un campione di N=3500 pazienti.
Criteri inclusione: Tutte le donne, con età superiore ai 18 anni, portatrici di una mutazione patogenetica di classe 4 e 5 della classificazione dell'Agenzia Internazionale di Ricerca sul Cancro) dei geni BRCA1 o BRCA2.
Criteri esclusione: Pazienti di età inferiore ai 18 anni - Mutazioni nei geni BRCA1/2 non patogenetiche.

2.3 TIPOLOGIA DI STUDIO

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

2.4 NUMERO DI PAZIENTI ARRUOLATI

10.000 pazienti totali di cui 6500 per la parte retrospettiva.

2.5 DATASET, PSEUDONIMIZZAZIONE, CONTROLLI DI INTEGRITÀ, DATA BREACH

- Riportare una riga di dataset (es. CRF)

Index Case, Sesso, Età menarca, Clinival Trials, Test genetico eseguito, Mutazione, Nomenclatura mutazione, Data test genetico, Centro, Motivo test, Note.

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

al momento dell'inserimento della paziente su REDCap, viene assegnato un codice univoco automatico costituito dal codice centro + numero progressivo (nel caso di FPG: 3061-1, 3061-2, 3061-3 ecc..).
Oltre a questo, c'è la possibilità di assegnare ad ogni paziente un codice specifico del centro che potrebbe essere utilizzato per la gestione dei dati a livello locale.
Per ottenere ciò, il data collection ha provveduto a sviluppare un file Excel che permette di generare lo Study ID Code da inserire nella eCRF per ciascun paziente.
Per generare il codice, una volta aperto il file, si inseriscono le iniziali della paziente, la data di nascita e si preme invio. Il codice generato potrà essere riportato in eCRF.

[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

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

La tabella di conversione è conservata esclusivamente in ambiente separato e sicuro, accessibile solo ai promotori dello studio o al centro coordinatore, con credenziali specifiche e accesso tracciato. Il database RedCap utilizzato per l'inserimento e la gestione dei dati pseudonimizzati non contiene i dati identificativi.

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

I dati possono essere modificati o aggiornati esclusivamente dagli investigatori registrati che li hanno inseriti o da altri utenti afferenti alla stessa Istituzione, previa autenticazione con credenziali personali. Il sistema RedCap implementa controlli automatici di validità dei campi (es. formato date, valori ammissibili).

- 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)

Il Principal Investigator ha informato e formato tutto il personale coinvolto attraverso:

-Sessioni di formazione specifica (in presenza o online) sui principi di sicurezza e gestione dei dati personali;
-Obbligo di comunicazione immediata al PI o al referente privacy del centro in caso di violazione o anomalia.

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	Inserimento, gestione e pseudonimizzazione dei dati clinici dello studio	FPG	open
2	TrakCare	Raccolta dati clinici, anamnestici e follow-up	FPG	InterSystems S.p.A.
3	IBM-SPSS	Software IBM commerciale, molto diffuso in ambito clinico e nelle scienze sociali per analisi statistiche.	FPG	IBM

2.7 CRF/ECRF

- In caso di eCRF indicare software/piattaforma utilizzata

La piattaforma utilizzata per la eCRF è REDCap (Research Electronic Data Capture).

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

I dati vengono inseriti direttamente dai centri sperimentatori nella piattaforma REDCap, tramite accesso sicuro e autenticato.

Ogni centro ha accesso esclusivo ai propri dati e a quelli della propria Istituzione.

Non è previsto uno scambio di file esterni: i dati restano centralizzati nella piattaforma e vengono esportati solo dal centro coordinatore per analisi aggregate.

- 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

NA. Lo studio utilizza esclusivamente eCRF (piattaforma REDCap); non è prevista la gestione o conservazione di CRF cartacee.

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

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

2.9 RUOLI PRIVACY

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

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

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

Lista Centri Partecipanti

Versione 3.0 del 20/03/2025

Prof.ssa Anna Fagotti	Policlinico Universitario Agostino Gemelli IRCCS (Promotore)
Dott.ssa Maria Cristina Petrella	AOU Careggi, Firenze
Prof. Tommaso Simoncini	Azienda Ospedaliera Universitaria Pisana, Pisa
Dott.ssa Dora Miano	Azienda Ospedaliera Universitaria Senese, Siena SI
Dott. Roberto Berretta	Azienda Ospedaliero Universitaria di Parma, Parma
Dott.ssa Martina Arcieri	Azienda Sanitaria Universitaria Friuli Centrale, Udine UD
Dott.sa Claudia Andreetta	Azienda Sanitaria Universitaria Friuli Centrale, Udine UD
Dott.ssa Elisa Picardo	Città della Salute e della Scienza di Torino - Ospedale S. Anna, Torino
Prof. Robert Fruscio	Fondazione IRCCS San Gerardo di Monza, Monza MB
Dott.ssa Gabriella Zito	I.R.C.C.S. Burlo Garofalo, Trieste
Dott.ssa Valentina Arcangeli	I.R.S.T. IRCCS, Meldola, Meldola FC
Dott.ssa Rosanna Mancari	IRCCS Istituto Nazionale Tumori Regina Elena, Roma RM
Dott.ssa Antonella Savarese	IRCCS Istituto Nazionale Tumori Regina Elena, Roma RM
Dott.ssa Chiara Cassani	IRCCS Policlinico S. Matteo, Pavia
Dott.ssa Jole Ventriglia	Istituto Nazionale Tumori Fondazione G. Pascale, Napoli NA
Dott.ssa Katia Cannita	Ospedale G. Mazzini di Teramo, Teramo
Dott.ssa Valentina Ceni	Ospedale Papa Giovanni XXIII Bergamo, Bergamo
Dott.ssa Teresa Di Palma	Ospedale S. Maria Goretti, Latina
Dott.ssa Emanuela Rabaiotti	Ospedale San Raffaele, Milano MI
Dott.ssa Daniela Sambataro	Ospedale Umberto I - ASP di Enna, Enna EN
Dott.ssa Elisabetta De Matteis	Ospedale Vito Fazzi, Lecce
Dott.ssa Alessandra Baldoni	Presidio Ospedaliero di Mirano, Mirano VE

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI

Prof.ssa Vera Loizzi	Università degli Studi di Bari "Aldo Moro", Bari
Dott.ssa Valentina Tuninetti	Università di Torino Ospedale Mauriziano Umberto I, Torino
Dott.ssa Lorena Incorvaia	Azienda Ospedaliera Universitaria Policlinico Paolo Giaccone
Dott.ssa Francesca Falcone	Clinica Malzoni, Avellino
Dott. Marco Marinaccio	Università degli Studi di Bari "Aldo Moro", Bari
Dott.ssa Amelia Barcellini	Centro Nazionale di Adroterapia Oncologica, Pavia
Dott.ssa Grazia Artioli	Azienda ULSS 2 MARCA TREVIGIANA
Dott. Stefano Bogliolo	PO del Tigullio ASL 4 Chiavarese Genova, Chiavari
Dott.ssa Angelica Sikokis	Azienda Ospedaliera Universitaria di Parma
Dott.ssa Lucia Trevisan	IRCCS Ospedale Policlinico San Martino
Dott.ssa Marinella De Stefanis	A.O. Santa Croce e Carle – Cuneo
Dott.ssa Giovanna Scarfone	Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico – Milano
Dott.ssa Margherita Turinetto	Humanitas San Pio X- Milano
Dott. Ivano Raimondo	Ospedale Mater Olbia– Olbia
Dott.ssa Innocenza Palaia	Policlinico Umberto I Università "La Sapienza" – Roma
Dott.ssa Veronica Parolin	Azienda Ospedaliera Universitaria Integrata - Verona
Prof. Paolo Scollo	Azienda Ospedaliera per l'emergenza Cannizzaro, Catania
Dott.ssa Lucia Borgato	AULSS 8 Berica, Vicenza
Dott. Antonino Ditto	Centro di ricerca oncologico (CRO) di Aviano, Pordenone

- **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	\	

E-MAIL: dpo@policlinicogemelli.it

- 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

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.

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:
- 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)

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

E-MAIL: dpo@policlinicogemelli.it

	• 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
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. 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
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.

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

Riservatezza – accesso illegittimo ai dati

E-MAIL: dpo@policlinicogemelli.it

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.

Firmata digitalmente da

Avv. Francesco Giorgianni

FRANCESCO GIORGIANNI
17/09/2025 18:39:50 UTC+0200

E-MAIL: dpo@policlinicogemelli.it

8. DOCUMENTI A SUPPORTO

omissis