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: 7296

NOME DELLO STUDIO: GIM-32

PRINCIPAL INVESTIGATOR: DOTT.SSA ANTONELLA PALAZZO

16/07/2026

Sommario

1. CONSIDERAZIONI PRELIMINARI 4

2. DESCRIZIONE DELLO STUDIO - Contesto, responsabilità, standard, risorse di supporto 5

2.1 Specificare ID e Titolo originale dello Studio 5
2.2 Sinossi dello Studio 5
2.3 Tipologia Di Studio 12
2.4 Numero Di Pazienti Arruolati 12
2.5 Dataset, Pseudonimizzazione, controlli di integrità, Data breach 12
2.6 Database E Software Utilizzati 14
2.7 CRF/eCRF 14
2.8 Campioni Biologici 15
2.9 Risorse: Soggetti interni coinvolti nello studio (ruoli e funzioni) 15
2.10 Ruoli Privacy 15

E-MAIL: dpo@policlinicogemelli.it

2.11 Trasferimenti dati extra UE 18

3. PRINCIPI FONDAMENTALI 19

3.1 PROPORZIONALITÀ E NECESSITÀ 19

3.11 Gli scopi del trattamento sono specifici, espliciti e legittimi? 19

3.12 Quali sono le basi legali che rendono lecito il trattamento? 19

3.13 Ci sono standard applicabili al trattamento? 19

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)? 21

3.15 I dati sono esatti e aggiornati? 21

3.16 Qual è il periodo di conservazione dei dati? 21

3.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI 22

3.21 Come sono informati del trattamento gli interessati? 22

3.22 Ove applicabile: come si ottiene il consenso degli interessati? 22

3.23 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati? 22

3.24 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)? 23

3.25 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione? 23

3.26 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto? 23

3.27 In caso di trasferimento di dati al di fuori dell'unione europea, i dati godono di una protezione equivalente? 24

4. CALCOLO DEL RISCHIO 24

5. ANALISI DEI RISCHI 25

5.1 Tabella delle Contromisure tecniche 25

5.2 Tabella delle Contromisure logistiche 26

5.3 Tabella delle Contromisure Organizzative 26

5.4 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? 27
5.5 Quali sono le principali minacce che potrebbero concretizzare il rischio? 28
5.6 Quali sono le fonti di rischio? 29
5.7 Quali misure fra quelle individuate contribuiscono a mitigare il rischio? 29
6. RISULTATI DPIA E AZIONI DI MIGLIORAMENTO 29
7. RISULTATI DPIA – PARERE DEL DPO 30
8. DOCUMENTI A SUPPORTO 30

ATTIVITA’	FUNZIONE	RESPONSABILE	DATA
Redatto da:	Ufficio Privacy	\	16/07/2026
Verificato da:	DPO	Avv. Giorgianni	
Firmato da:	PI	DOTT.SSA ANTONELLA PALAZZO	\

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

1. CONSIDERAZIONI PRELIMINARI

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

L'art. 44 comma 1 bis della legge 29 aprile 2024, n. 56 ha modificato l'art. 110 del Codice della privacy eliminando il requisito dell'autorizzazione preventiva del Garante, ove, per finalità di ricerca medico – scientifica, sia necessario utilizzare dei dati per i quali non è più possibile ottenere il consenso. Il nuovo art. 110 del Codice della privacy, infatti, prevede che: "Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice".
Inoltre, come riportato nelle FAQ succitate: "***Gli IRCCS possono**, in alternativa* [al consenso, n.d.R], ***fondare il trattamento dei dati personali raccolti per scopi di cura per ulteriori finalità di ricerca in campo medico, biomedico e epidemiologico sull'art. 110-bis**, comma 4 del Codice, in base al quale "Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento".*
L'art. 110-bis, comma 4 del Codice costituisce una di quelle disposizioni di legge, che si inseriscono nello spazio di normazione lasciato agli Stati membri, ai sensi dell'art. 9, par. 2, lett. j) del Regolamento, alle quali fa riferimento l'art. 110 (primo comma, primo periodo) del Codice nella parte in cui prevede che: "1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, [...] ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento"."

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

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

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: 7296

Titolo: Beneficio della terapia adiuvante nel carcinoma mammario in premenopausa in accordo al test Oncotype DX

2.2 SINOSSI DELLO STUDIO

SINOSSI

TITOLO DELLO STUDIO	Beneficio della terapia adiuvante nel carcinoma mammario in premenopausa in accordo al test Oncotype DX
ACRONIMO	GIM32-PERSEVERE-X
PROMOTORE	Fondazione Policlinico A. Gemelli, IRCCS L.go Francesco Vito 1, 00168 Roma
CRO	Clinical Research Technology
COFINANZIATORE	Exact Sciences
SPERIMENTATORE PRINCIPALE	Dott.ssa Antonella Palazzo UOC Oncologia Medica
BACKGROUND E RAZIONALE DELLO STUDIO	L'incidenza del cancro al seno aumenta con l'età fino alla settima decade di vita. Tra il 2015-2019, l'età media alla diagnosi di cancro al seno è stata di 62 anni. La probabilità di diagnosi di cancro al seno nelle donne più giovani (≤ 40 anni) è di circa il 3,2% [1]. Il processo decisionale clinico riguardante l'uso del trattamento adiuvante per il carcinoma mammario invasivo in fase iniziale (eBC) si basa in gran parte su una varietà di fattori, tra cui lo stadio anatomico, le caratteristiche biologiche del cancro e le caratteristiche del paziente. La scelta del trattamento

E-MAIL: dpo@policlinicogemelli.it

adiuvante rappresenta una sfida importante, soprattutto nei eBC a recettori ormonali positivi (HR+)/HER2-negativi (HER2-) a rischio intermedio, dove il beneficio aggiuntivo della chemioterapia (CT) rispetto all'uso della sola terapia endocrina (ET) è in gran parte poco chiaro. Nelle pazienti con carcinoma mammario HR+/HER2-, i pannelli multigenici che identificano le mutazioni espresse dal tessuto tumorale possono aiutare a guidare la pratica terapeutica. Il test Oncotype DX (ODX) valuta 21 geni per determinare il rischio di recidiva della malattia dopo il trattamento nel carcinoma mammario in fase iniziale HR+/HER2−. Questo test è stato validato specificatamente in pazienti con stadiazione T1-T3, N0-N1 e M0. I pazienti identificati come ad alto rischio di recidiva beneficiano del trattamento sistemico che combina chemioterapia e terapia endocrina (terapia chemio-endocrina, CET) rispetto alla sola terapia endocrina (ET). Mentre per le pazienti in menopausa, i dati di letteratura sono inequivocabili e dimostrano che la chemioterapia può essere omessa in pazienti con RS <26, riducendo al minimo l'esposizione non necessaria al trattamento citotossico, le linee guida per il trattamento delle pazienti in premenopausa raccomandano criteri più stringenti per il ruolo predittivo del test genomico, in accordo allo stato linfonodale. Nello studio TAILORx [3], che studiava il ruolo del beneficio della chemioterapia adiuvante nelle pazienti con cancro al seno HR+/HER2- con linfonodi negativi, tra donne di età pari o inferiore a 50 anni, la maggior parte delle quali era in premenopausa e trattata con tamoxifene da solo o seguita sequenzialmente con un farmaco aromatasi inibitore, il tasso di recidiva a distanza a 9 anni era inferiore al 5% (≤1,8±0,9%) tra quelli con un basso punteggio di rischio di recidiva (recurrence score, RS), indipendentemente dal rischio clinico e un punteggio di recidiva intermedio con basso rischio clinico (4,7 ± 1,0%). Al contrario, il tasso di recidiva a distanza a 9 anni ha superato il 10% tra le donne con alto rischio clinico e un punteggio di recidiva intermedio che hanno ricevuto la sola terapia endocrina (12,3±2,4%) e in quelle con un punteggio di recidiva elevato che hanno ricevuto la terapia chemio-endocrina (15,2±3,3%). Nello studio RxPONDER [4], che ha

valutato pazienti con cancro al seno con linfonodi positivi (1-3 linfonodi), le donne in premenopausa hanno ottenuto un maggiore beneficio di sopravvivenza libera da malattia invasiva (iDFS) con l'aggiunta di CT, indipendentemente dal valore di RS (intervallo 0-25) e il numero di linfonodi coinvolti (intervallo 1–3).

Nonostante queste evidenze, non è chiaro se il beneficio identificato nello studio RxPONDER di un minor rischio di recidiva a distanza anche in pazienti con RS < 26 o in pazienti con malattia a linfonodi negativi, intermedio RS e alto rischio clinico, fosse dovuto all'effetto di soppressione ovarica della chemioterapia, rappresentando un'importante area di ricerca.

Nel 78% delle pazienti incluse nello studio TailorX la terapia endocrina ricevuta era rappresentata dal tamoxifene in monoterapia (di cui il 35% ha ricevuto uno switch ad inibitore dell'aromatasi) o in associazione alla soppressione della funzione ovarica; il 13% delle pazienti in premenopausa arruolate nello studio ha ricevuto una combinazione di inibitore dell'aromatasi in associazione alla soppressione ovarica. Lo studio TAILORx ha riportato un chiaro vantaggio della CT rispetto alla ET in quelle pazienti giovani che hanno ottenuto la menopausa precoce. Di conseguenza, per le pazienti di età compresa tra 46 e 50 anni è stato dimostrato un beneficio maggiore rispetto a quelle di età avanzata, suggerendo che l'amenorrea indotta dalla chemioterapia gioca un ruolo più rilevante rispetto all'effetto citotossico diretto della CT in una condizione di soppressione ovarica (OFS) stabilita, come previsto nelle donne in perimenopausa (46-50 anni).

Nei due studi TEXT e SOFT [7] è stato dimostrato un miglioramento del 5% nei tassi di recidiva per le pazienti in premenopausa HR+/HER2- trattate con OFS in aggiunta all'ET standard, con un tasso fino al 10% miglioramento assoluto della sopravvivenza libera da recidiva (RFS) a 8 anni. Pertanto, è possibile che l'uso di strategie di trattamento endocrino più potenti del tamoxifene, come l'OFS in associazione ad un inibitore dell'aromatasi (AI), potrebbe fornire benefici paragonabili alla CT. Risultati simili sono stati riscontrati nello studio NSABP B-30, che ha

mostrato miglioramenti sia in termini di OS che di DFS tra le donne in premenopausa che hanno manifestato amenorrea indotta da chemioterapia (CIA) per almeno sei mesi dopo la TC adiuvante. Inoltre, i risultati degli studi preoperatori ADAPT e ADPT-cycle [5-6] sembrano aver raggiunto conclusioni simili. E' stato, difatti, osservata una maggior risposta alla terapia ET (Ki67 <10%) nelle pazienti in premenopausa in entrambi i gruppi di RS (0-25 e ≥26) quando l'OFS è stata aggiunto al solo ET. L'analisi ha anche mostrato che nel gruppo più controverso di pazienti in premenopausa di età inferiore a 40 anni, la risposta ET con AI più OFS era fino all'85% in RS 0-25 e al 60% in RS ≥ 26, supportando l'ipotesi di poter omettere la CT a favore di OFS più ET nella maggior parte dei pazienti giovani, N1, con eBC in base al rischio clinico e genomico e responsive alla ET preoperatoria.
Le linee guida sul cancro al seno dell'Associazione Italiana Oncologia (AIOM) per il trattamento endocrino adiuvante raccomandano fortemente di considerare l'uso dell'analogo dell'LHRH nelle pazienti in premenopausa ad alto rischio di recidiva [2].
Questi dati, oltre che più alto è il RS e maggiore è il beneficio del CT, suggeriscono che ET in associazione ad OFS può rappresentare una valida opzione terapeutica per le donne più giovani con RS < 25.
Lo scopo di questo studio è quello di indagare maggiormente l'impatto dei trattamenti adiuvanti (ET con o senza OFS; CET) nelle pazienti in premenopausa HR+/HER2- in base al loro rischio genomico.

OBIETTIVI DELLO STUDIO

Primario: descrivere l'outcome del trattamento adiuvante nelle pazienti con carcinoma mammario a recettori ormonali positivi, HER 2 negativi in premenopausa con linfonodi negativi (pN0) e/o linfonodi positivi (pN1-3) in base al loro rischio genomico.

Secondari: descrivere l'effetto del tipo di trattamento adiuvante (chemioterapia/terapia endocrina; terapia endocrina con o senza OSF) nelle pazienti con carcinoma

	mammario a recettori ormonali positivi, HER2 negativi in premenopausa pN0 e pN1 in base al loro rischio genomico.
ENDPOINT	**Primari**: sopravvivenza libera da malattia invasiva (iDFS) a 5 anni nei gruppi di pazienti affette da carcinoma mammario a recettori ormonali positivi, HER2 negativi pN0 e pN1, in accordo al loro rischio genomico valutato mediante Oncotype DX. **Secondari**: correlare la iDFS a 5 anni con il trattamento adiuvante ricevuto (chemio-endocrino terapia; terapia endocrina in associazione o meno alla soppressione ovarica) lo stato patologico del tumore ed il rischio genomico valutato mediante Oncotype DX.
DISEGNO DELLO STUDIO	Studio osservazionale ambispettico, multicentrico
NUMERO DI PAZIENTI	800
POPOLAZIONE TARGET	Pazienti in premenopausa affette da carcinoma mammario a recettori ormonali positivi HER2 negativi in stadio precoce sottoposte al test 21-multigene Oncotype DX tra il 1 gennaio 2013 e il 31 dicembre 2022 e successiva terapia adiuvante. Verrà richiesto il consenso informato per i pazienti arruolati prospetticamente, mentre per quelli arruolati retrospettivamente si farà riferimento all'art. 110-bis del Codice Privacy.
CRITERI DI INCLUSIONE	1. Pazienti di sesso femminile, in premenopausa e di età ≥ 18 anni; 2. consenso informato per i pazienti arruolati prospetticamente, mentre per quelli arruolati retrospettivamente si farà riferimento all'art. 110-bis del Codice Privacy. 3. Diagnosi istologica di cancro al seno in fase iniziale positivo per i recettori ormonali ER e/o PgR HER2 negativo. 4. Stadio linfonodale patologico pN0 o pN1 (1-3 linfonodi) e stadio tumorale patologico da pT1 a pT3.

E-MAIL: dpo@policlinicogemelli.it

	5. Tutti i pazienti sottoposti a intervento chirurgico per carcinoma mammario primario e stadiazione ascellare mediante biopsia del linfonodo sentinella o dissezione del linfonodo ascellare (ALND). 6. Disponibilità dei risultati del test Oncotype DX eseguito dal 1 gennaio 2013 al 31 dicembre 2022 su scelta del scelta del medico referente; 7. Disponibilità di informazioni cliniche e patologiche 8. Disponibilità di trattamenti adiuvanti ricevuti 9. Disponibilità delle informazioni di sopravvivenza del paziente (recidiva, sede della recidiva, sopravvivenza).
CRITERI DI ESCLUSIONE	1. Evidenza di metastasi a distanza alla diagnosi iniziale 2. Cancro al seno infiammatorio 3. Sono escluse le pazienti sottoposte a trattamento neoadiuvante 4. pazienti non sottoposte a chirurgia mammaria o ascellare 5. Pazienti non testati per test Oncotype DX
DURATA DELLO STUDIO	Durata complessiva dello studio: 30 mesi circa Attivazione centri partecipanti: 12 mesi Durata dell'arruolamento: 12 mesi Analisi dei dati: 6 mesi circa
Trattamento dei dati personali ai sensi dell'art. 110-bis del Codice Privacy	Il Promotore ha provveduto a eseguire una Valutazione d'Impatto sulla protezione dei dati (DPIA), mediante la quale è stata accertata l'adeguatezza delle misure tecniche e organizzative adottate, al fine di garantire la tutela dei diritti e delle libertà fondamentali degli interessati, in conformità all'art. 89 del Regolamento (UE) 2016/679 e alle indicazioni del Garante per la protezione dei dati personali. Il trattamento dei dati sarà circoscritto alle finalità dello studio e condotto secondo i principi di minimizzazione, pseudonimizzazione e sicurezza, nel rispetto delle garanzie definite dall'Autorità Garante in materia. L'estratto della DPIA è pubblicato sul sito web del Promotore e dei centri di sperimentazione.
ANALISI STATISTICA e dimensionamento campionario se applicabile	Si ipotizza di trovare tre diversi gruppi di trattamenti adiuvanti ricevuti in base ai gruppi di RS del test Oncotype DX (CET; ET+OFS; ET) per entrambe le coorti (linfonodi

E-MAIL: dpo@policlinicogemelli.it

	negativi e linfonodi positivi). Tenendo conto dei risultati derivanti dai due studi precedenti prospettici (studi RxPONDER e TAILORx), si ipotizza di osservare nella popolazione oggetto di questo studio una iDFS a 5 anni di circa il 90% per la popolazione complessiva arruolata nello studio (N0 e N1). 800 pazienti permetteranno di stimare questo tasso con un intervallo di confidenza al 95% di ampiezza pari a 4 % (es. 88%-92%).
SICUREZZA/GESTIONE REGOLATORIA DEGLI EVENTI AVVERSI	Tutti gli eventi avversi saranno raccolti, registrati e valutati per gravità e relazione con i prodotti medicinali in studio e non, ai fini dell'identificazione di sospette reazioni avverse. Ogni sospetta reazione avversa osservata per lo studio prospettico sarà segnalata all'Autorità Nazionale Competente - AIFA, a prescindere dalla gravità, secondo il flusso di farmacovigilanza post marketing, previsto da DM 30 aprile 2015 e GVP (Good Vigilance Practices) modulo VI, mediante comunicazione al Responsabile Locale di Farmacovigilanza ai fini dell'inserimento in Rete Nazionale di Farmacovigilanza e, laddove previsto, al Comitato Etico. Per lo studio retrospettivo con analisi secondaria dei dati, non sussiste obbligo di segnalazione di sospette reazioni avverse, essendo state eventualmente le stesse già a suo tempo comunicate secondo quanto previsto da DM 30.04.2015 e GVP modulo VI sez. C.1.2.1.2.
DOCUMENTO DI RIFERIMENTO PER LA SICUREZZA	RCP (Riassunto delle caratteristiche del prodotto)
BIBLIOGRAFIA	1. American Cancer Society Breast cancer fact and figures, 2022-2024 2. AIOM: linee guida tumore della mammella. Versione 16 settembre 2015 3. Sparano JA et al. Clinical and Genomic Risk to Guide the Use of Adjuvant Therapy for Breast Cancer. N Engl J Med 2019; 380:2395-2405 4. Kalinski K. Et al. 21-Gene Assay to Inform Chemotherapy Benefit in Node-Positive Breast Cancer. N Engl J Med 2021; 385:2336-2347 5. Harbeck, N. et al. ADAPTcycle: Adjuvant dynamic marker-adjusted personalized therapy (ADAPT) comparing endocrine therapy plus ribociclib versus

chemotherapy in intermediate-risk HR+/HER2- early breast cancer (EBC). JCO 2020, 38, TPS601

6. Gluz, O.U.A. et al. LBA14—Impact of age, recurrence score (RS) and ovarian function suppression (OFS) on endocrine response to short preoperative endocrine therapy (ET): Analysis of ADAPT and ADAPTcycle trials. Ann. Oncol. 2022, 33, S808–S869.
7. Pagani O, Walley BA, Fleming GF,et al. Adjuvant Exemestane With Ovarian Suppression in Premenopausal Breast Cancer: Long-Term Follow-Up of the Combined TEXT and SOFT Trials. J Clin Oncol. 2023 Mar 1;41(7):1376-1382.

2.3 TIPOLOGIA DI STUDIO

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

2.4 NUMERO DI PAZIENTI ARRUOLATI

800 pazienti

2.5 DATASET, PSEUDONIMIZZAZIONE, CONTROLLI DI INTEGRITÀ, DATA BREACH

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

[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).

Il software utilizza algoritmi avanzati per la pseudonimizzazione automatica dei dati personali. I dati identificativi vengono sostituiti con codici univoci generati automaticamente al momento dell'inserimento nel sistema.

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

  I dati identificativi vengono conservati in un database separato rispetto ai dati clinici, accessibile solo a personale autorizzato, limitando l'accesso solo a chi ha necessità operative specifiche. L'accesso ai dati è consentito esclusivamente a utenti autorizzati mediante credenziali personali univoche e profili di autorizzazione basati su ruoli, applicando il principio del minimo privilegio.

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

  Controlli di validazione dei dati:
  Il sistema implementa controlli di validazione applicativa per garantire che i dati inseriti siano accurati, coerenti e completi, riducendo il rischio di errori o alterazioni non autorizzate.
  Verifica dell'integrità dei dati:
  Sono adottati meccanismi tecnici e procedurali per garantire l'integrità dei dati durante la trasmissione e la memorizzazione, anche attraverso controlli applicativi e sistemi di tracciabilità.
  Inoltre, il database utilizzato dalla piattaforma eClinical è di tipo transazionale: le operazioni di scrittura vengono confermate solo al completamento corretto della transazione; in caso contrario, i dati non vengono salvati, garantendo così l'integrità delle informazioni.
  Audit trail:
  Tutte le modifiche ai dati sono registrate tramite audit trail, con indicazione di data, ora e utente che ha effettuato l'operazione, garantendo la completa tracciabilità e la possibilità di revisione delle modifiche.

- **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)**
  L'accesso al sistema è consentito esclusivamente a utenti autorizzati mediante credenziali personali univoche.
  Sono implementati ruoli e permessi basati sulle mansioni e sul principio del minimo privilegio.
  Il sistema supporta meccanismi di autenticazione a più fattori (MFA).
  Gli accessi e le operazioni effettuate sono monitorati e registrati al fine di individuare attività sospette o non autorizzate.
  Formazione del personale:

Il personale coinvolto nel trattamento dei dati riceve formazione periodica in materia di sicurezza delle informazioni, riservatezza e protezione dei dati personali.

2.6 DATABASE E SOFTWARE UTILIZZATI

PACS, TrakCare SI-trial per FPG, mentre per gli altri centri cartella clinica

- 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	eClinical	eCRF	Piattaforma online	Clinical Research Technology Srl
2	SPSS	Analisi statistica	FPG	FPG

I software utilizzati elaborano i dati solo in modalità locale e il produttore/fornitore non ha contratti di manutenzione per cui non entra in alcun modo in contatto con i dati trattati attraverso tali software.

2.7 CRF/ECRF

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

eClinical

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

è di fornitore esterno

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

Clinical Research Technology Srl

E-MAIL: dpo@policlinicogemelli.it

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

ogni centro, dopo l'attivazione, avrà accesso tramite le credenziali fornite allo staff di studio alla piattaforma eCRF eClinical

- **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

2.8 CAMPIONI BIOLOGICI

- Campioni conservati nella biobanca di FPG e trattati in FPG

☐ SI
☒ NO

- Campioni inviati a biobanche o centri esterni per specifiche analisi

☐ SI
☒ NO

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.

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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

	Autonomi titolari	Indirizzo
	Fondazione Policlinico Universitario Agostino Gemelli IRCCS, (P.I. Palazzo)	Largo Francesco Vito 1, 00168 Roma
	Nuovo Ospedale Santo Stefano	Via Suor Niccolina Infermiera, 20/22, Prato 59100
	IRCCS Ospedale Policlinico S. Martino,	Largo Rosanna Benzi, 10 Genova 16132
	Ospedale Riuniti di Ancona	Via Conca, 71 Ancona 60126
	Azienda Ospedaliero Universitaria di Modena	Via del Pozzo, 71 Modena 41124
	IRCCS Ospedale San Raffaele	Via Olgettina, 60 Milano 20132
	ASST Fatebenefratelli Sacco	Via G.B. Grassi, 74 Milano 20157
	Azienda Ospedaliera Universitaria Integrata Verona	Piazzale Aristide Stefani 1 Verona 37126
	Centro di riferimento Oncologico	Via Franco Gallini n.2 Aviano 33081
	Istituto Romagnolo per lo Studio dei Tumori "Dino Amadori" - IRST IRCCS	Via Piero Maroncelli, 40 Meldola 47014
	Istituto Nazionale Tumori Regina Elena	Via Elio Chianesi, 53 Roma 00144
	Fondazione IRCCS Istituto Nazionale dei Tumori	Via Giacomo Venezian, 1 Milano 20133
	Policlinico Universitario Campus Bio-Medico	Via Alvaro del Portillo, 200 Roma 00128
	Presidio di Brindisi "Di Summa - Perrino"	Strada Statale 7 per Mesagne, Brindisi 72100
	ASST Papa Giovanni XIII	Piazza OMS, 1 Bergamo 24127
	Azienda Ospedaliero Universitaria Pisana	Via Roma, 67 Pisa 56126

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

	Fondazione Policlinico Universitario Agostino Gemelli IRCCS, (P.I. Fabi)	Largo Francesco Vito 1, 00168 Roma
	AOU Federico II	Via Sergio Pansini, 5 Napoli 80131
	AOU Policlinico Umberto I	Viale del Policlinico, 155 Roma 00155
	AOU Maggiore della Carità	Corso Giuseppe Mazzini, 18 Novara 28100
	Azienda Ospedaliera Universitaria "P. Giaccone'	Via del Vespro, 129 Palermo 90127
	AOU Careggi	Largo Brambilla, 3 Firenze 50134
	ASL Roma 1 - Ospedale Santo Spirito	Lungotevere in Sassia, 1 Roma 00193
	Fondazione IRCCS San Gerardo	Via Pergolesi, 33 Monza 20900

- **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	eClinical	Clinical Research Technology Srl	Via San Leonardo trav. Migliaro 84131 Salerno (Italy)

  - Contract Research Organization (CRO) ☒ SI ☐ NO

E-MAIL: dpo@policlinicogemelli.it

Se sì, specificare Nome, indirizzo e PEC della CRO

Clinical Research Technology Srl , Via San Leonardo trav. Migliaro 84131 Salerno (Italy)

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

	Nome laboratorio	Indirizzo	Ruolo Privacy
1	\		

2.11 TRASFERIMENTI DATI EXTRA UE

I dati sono trasferiti extra UE

☐ SI ☒ NO

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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);

E-MAIL: dpo@policlinicogemelli.it

- 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			

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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			

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

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.

E-MAIL: dpo@policlinicogemelli.it

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

E-MAIL: dpo@policlinicogemelli.it

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 • 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

E-MAIL: dpo@policlinicogemelli.it

	• 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	Il trattamento dei dati personali avviene solo tramite dispositivi/ personal computer aziendali

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

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.**
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.

E-MAIL: dpo@policlinicogemelli.it

Fondazione Policlinico Universitario Agostino Gemelli IRCCS
Università Cattolica del Sacro Cuore

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.

Approvato dal DPO

Avv. Francesco Giorgianni

8. DOCUMENTI A SUPPORTO

omissis

E-MAIL: dpo@policlinicogemelli.it