



## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### DATA PROTECTION IMPACT ASSESSMENT STUDI CLINICI

#### ESTRATTO

ID DELLO STUDIO: 8165

NOME DELLO STUDIO: DARE

PRINCIPAL INVESTIGATOR: CAMILLA NERO

18/02/2026

## Sommario

|                                                                                              |          |
|----------------------------------------------------------------------------------------------|----------|
| <b>1. CONSIDERAZIONI PRELIMINARI .....</b>                                                   | <b>4</b> |
| <b>2. DESCRIZIONE DELLO STUDIO - Contesto, responsabilità, standard, risorse di supporto</b> | <b>5</b> |
| 2.1 Specificare ID e Titolo originale dello Studio.....                                      | 5        |
| 2.2 Sinossi dello Studio.....                                                                | 5        |
| 2.3 Tipologia Di Studio .....                                                                | 10       |
| 2.4 Numero Di Pazienti Arruolati.....                                                        | 11       |
| 2.5 Dataset, Pseudonimizzazione, controlli di integrità, Data breach.....                    | 11       |
| 2.6 Database E Software Utilizzati .....                                                     | 14       |
| 2.7 CRF/eCRF .....                                                                           | 15       |
| 2.8 Campioni Biologici .....                                                                 | 15       |
| 2.9 Risorse: Soggetti interni coinvolti nello studio (ruoli e funzioni).....                 | 16       |
| 2.10 Ruoli Privacy.....                                                                      | 16       |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|            |                                                                                                                                                              |           |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 2.11       | Trasferimenti dati extra UE.....                                                                                                                             | 18        |
| <b>3.</b>  | <b>PRINCIPI FONDAMENTALI .....</b>                                                                                                                           | <b>18</b> |
| <b>3.1</b> | <b>PROPORZIONALITÀ E NECESSITÀ .....</b>                                                                                                                     | <b>18</b> |
| 3.11       | Gli scopi del trattamento sono specifici, espliciti e legittimi? .....                                                                                       | 18        |
| 3.12       | Quali sono le basi legali che rendono lecito il trattamento? .....                                                                                           | 18        |
| 3.13       | Ci sono standard applicabili al trattamento? .....                                                                                                           | 18        |
| 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)? ..... | 20        |
| 3.15       | I dati sono esatti e aggiornati? .....                                                                                                                       | 20        |
| 3.16       | Qual è il periodo di conservazione dei dati? .....                                                                                                           | 20        |
| <b>3.2</b> | <b>MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI.....</b>                                                                                                    | <b>21</b> |
| 3.21       | Come sono informati del trattamento gli interessati? .....                                                                                                   | 21        |
| 3.22       | Ove applicabile: come si ottiene il consenso degli interessati? .....                                                                                        | 21        |
| 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)? .....                                            | 22        |
| 3.25       | Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione? .....                                                                | 22        |
| 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? .....                                         | 23        |
| <b>4.</b>  | <b>CALCOLO DEL RISCHIO .....</b>                                                                                                                             | <b>23</b> |
| <b>5.</b>  | <b>ANALISI DEI RISCHI .....</b>                                                                                                                              | <b>24</b> |
| 5.1        | Tabella delle Contromisure tecniche .....                                                                                                                    | 24        |
| 5.2        | Tabella delle Contromisure logistiche .....                                                                                                                  | 25        |
| 5.3        | Tabella delle Contromisure Organizzative .....                                                                                                               | 26        |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|           |                                                                                                             |           |
|-----------|-------------------------------------------------------------------------------------------------------------|-----------|
| 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? .....                             | 27        |
| 5.6       | Quali sono le fonti di rischio? .....                                                                       | 28        |
| 5.7       | Quali misure fra quelle individuate contribuiscono a mitigare il rischio? .....                             | 28        |
| <b>6.</b> | <b>RISULTATI DPIA E AZIONI DI MIGLIORAMENTO .....</b>                                                       | <b>29</b> |
| <b>7.</b> | <b>RISULTATI DPIA – PARERE DEL DPO.....</b>                                                                 | <b>29</b> |
| <b>8.</b> | <b>DOCUMENTI A SUPPORTO .....</b>                                                                           | <b>29</b> |

| ATTIVITA'      | FUNZIONE        | RESPONSABILE    | DATA       |
|----------------|-----------------|-----------------|------------|
| Redatto da:    | Ufficio Privacy |                 | 18/02/2026 |
| Verificato da: | DPO             | Avv. Giorgianni |            |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 1. CONSIDERAZIONI PRELIMINARI

Questo modello di DPIA è implementato dalla Fondazione Policlinico Gemelli IRCCS per adempiere a quanto previsto dalle indicazioni del GDPR del 6 giugno 2016 *“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 2017, n. 56.

L’art. 44 comma 1 bis della legge 29 aprile 2017, 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 GDPR 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.”*

## 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

Titolo: Analisi del ctDNA per la valutazione della malattia minima residua nel carcinoma ovarico epiteliale in stadio iniziale: studio di fattibilità.

Acronimo: DARE

ID STUDIO: 18164

ID CENTRO: 20865

ID CINECA: 8165

#### 2.2 SINOSSI DELLO STUDIO

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TITOLO DELLO STUDIO</b>                 | Analisi del ctDNA per la valutazione della malattia minima residua nel carcinoma ovarico epiteliale in stadio iniziale: studio di fattibilità (DARE)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>ACRONIMO</b>                            | DARE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>PROMOTORE</b>                           | Fondazione Policlinico Universitario Agostino Gemelli IRCCS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>CRO</b>                                 | N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Cofinanziatore</b>                      | Fondazione AIRC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>SPERIMENTATORE PRINCIPALE</b>           | Camilla Nero, MD PhD<br>UOC di Ginecologia Oncologica                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>BACKGROUND E RAZIONALE DELLO STUDIO</b> | L'attuale standard terapeutico per le pazienti con carcinoma ovarico epiteliale (EOC) in stadio precoce è un intervento chirurgico di stadiazione completa che comprende una linfadenectomia sistematica pelvica e lombo-aortica seguita da chemioterapia a base di platino per le pazienti ad alto rischio. È stato riportato che la chemioterapia adiuvante aumenta la sopravvivenza libera da recidiva (RFS) a 5 anni di oltre il 10%, dal 65% al 76%, suggerendo quindi che 100 pazienti dovrebbero essere trattati per prevenire 12 recidive. Inoltre, il ruolo della chemioterapia rimane controverso nei pazienti con stadiazione ottimale, dove l'analisi dei sottogruppi non riporta un chiaro beneficio in termini di sopravvivenza globale (OS) con il trattamento adiuvante. Un precedente studio sul ruolo della dissezione del linfonodo sentinella nell'EOC in stadio precoce |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | <p>(NCT03563781) ha dimostrato che il 35% dei pazienti con linfonodi positivi è stato identificato solo con il protocollo di ultra-stadiazione sui linfonodi sentinella, suggerendo la necessità di una valutazione più accurata della malattia residua minima (MRD) dopo la stadiazione chirurgica. Sono stati segnalati biomarcatori prognostici basati sui tessuti nell'EOC in fase iniziale, ma sono ancora lontani dall'essere introdotti di routine nella pratica clinica. Inoltre, la nostra precedente esperienza sull'actionability basata sul NGS nell'EOC in fase iniziale ha dimostrato che il 70% dei pazienti presentava almeno un'alterazione potenzialmente actionable (ESCAT Tier I-III). La maggior parte dei pazienti che hanno sperimentato una recidiva della malattia nel nostro dataset apparteneva alla classe ad alto rischio, dove il tasso di alterazioni azionabili era del 51%, aprendo la strada all'integrazione della terapia mirata all'approccio standard in questa classe. In questo contesto, il DNA tumorale circolante (ctDNA) sta emergendo come un potente strumento per l'individuazione e il monitoraggio della MRD che potrebbe causare una recidiva in futuro. I risultati di studi condotti su altri tipi di tumore ne confermano il valore prognostico dopo un intervento chirurgico curativo, e una revisione sistematica incentrata sull'applicazione del ctDNA nell'EOC ha dimostrato che il ctDNA era significativamente associato a una peggiore sopravvivenza libera da progressione e OS. Nel numero limitato di casi in fase iniziale studiati, il ctDNA era rilevabile in circa il 60% dei casi preoperatori. Tuttavia, l'efficacia del ctDNA nella valutazione della MRD nei pazienti con EOC in fase iniziale dopo l'intervento chirurgico rimane incerta e attualmente non esistono studi registrati che valutino l'uso del rilevamento del ctDNA per l'approccio terapeutico nel contesto del trattamento adiuvante.</p> |
| <b>OBIETTIVI DELLO STUDIO</b> | <p>Abbiamo progettato uno studio retrospettivo per valutare la fattibilità dell'uso del ctDNA per rilevare la MRD sia nell'OC epiteliale in fase iniziale che in quella avanzata. Abbiamo pianificato di eseguire una valutazione retrospettiva dei livelli di ctDNA utilizzando campioni di plasma. Tutti i campioni che saranno utilizzati per questo studio sono conservati nella nostra Biobanca istituzionale e sono stati precedentemente raccolti (gennaio 2022 – settembre 2025) nell'ambito di altri studi.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>ENDPOINT</b>               | <p><b>endpoint primario:</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | <p>L'endpoint primario misura la clearance del ctDNA attraverso una valutazione binaria del ctDNA prima (T0) e dopo l'intervento chirurgico (T1).</p> <p><b>endpoint secondari:</b></p> <ul style="list-style-type: none"> <li>• Correlazione tra i livelli di ctDNA e le caratteristiche clinico-patologiche (grado, istologia, stadio)</li> <li>• Correlazione tra lo stato del ctDNA e la sopravvivenza libera da progressione (PFS)</li> </ul>    |
| <b>DISEGNO DELLO STUDIO</b>               | Monocentrico, retrospettivo, osservazionale, no profit cofinanziato                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>POPOLAZIONE TARGET</b>                 | Pazienti con carcinoma ovarico epiteliale in stadio iniziale e avanzato.                                                                                                                                                                                                                                                                                                                                                                              |
| <b>CRITERI DI INCLUSIONE</b>              | <ul style="list-style-type: none"> <li>• Carcinoma ovarico epiteliale (eccetto istotipo mucinoso)</li> <li>• Disponibilità di campioni plasmatici appaiati pre-operatori e post-operatori (4–7 settimane dopo l'intervento)</li> <li>• Volume minimo di 4 ml di plasma per ciascun timepoint</li> <li>• Stadio FIGO 2014 I–IV candidati a chirurgia con intento curativo (assenza di malattia macroscopicamente residua dopo l'intervento)</li> </ul> |
| <b>CRITERI DI ESCLUSIONE</b>              | <ul style="list-style-type: none"> <li>• Assenza di dati clinici</li> <li>• Follow-up inferiore a 6 mesi dall'intervento chirurgico</li> <li>• Diagnosi di altre neoplasie nei 5 anni precedenti</li> </ul> <p>Assenza di uno o entrambi i punti temporali prestabiliti</p>                                                                                                                                                                           |
| <b>DURATA DELLO STUDIO</b>                | 12 mesi                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>TRATTAMENTO/PROCEDURA SPERIMENTALE</b> | Il presente studio di fattibilità prevede l'analisi del ctDNA per la valutazione della malattia minima residua in pazienti affette da carcinoma ovarico epiteliale in stadio iniziale. L'analisi prevede l'utilizzo di campioni di sangue precedentemente raccolti nell'ambito di altri studi e conservati presso la Biobanca Istituzionale. L'analisi verrà effettuata dai laboratori Guardant Health (Palo Alto, CA 94304, USA).                    |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>ANALISI STATISTICA e dimensionamento campionario se applicabile</b></p>              | <p>ei campioni di sangue pre-chirurgici (T0) saranno confrontati con quelli raccolti 4 settimane dopo l'intervento (T1) per valutare i cambiamenti nel ctDNA e determinare la clearance del ctDNA. La variabile primaria è binaria (ctDNA rilevabile vs non rilevabile); le proporzioni appaiate saranno confrontate con il test di McNemar. Una coorte di 50 pazienti fornisce un errore standard massimo del 7%, equivalente a un intervallo di confidenza del 95% non superiore a <math>\pm 14\%</math>, ed è adeguata per esplorare le relazioni con gli esiti oncologici. Tutte le variabili dello studio saranno analizzate utilizzando statistiche descrittive. I dati categoriali saranno riportati come conteggi e percentuali, mentre i dati continui saranno valutati per la normalità (test di Shapiro-Wilk) e descritti come media (<math>\pm</math> SD) o mediana (IQR). Le variabili continue appaiate saranno testate utilizzando test t o, se non normali, il test di Wilcoxon per i dati continui. Le associazioni tra clearance del ctDNA, caratteristiche clinico-patologiche (grado, istologia, stadio) e PFS saranno esaminate utilizzando la regressione logistica per l'endpoint binario e modelli di rischio proporzionale di Cox per i dati relativi al tempo di evento, supportati dalle curve di Kaplan-Meier e dal test del log-rank. L'analisi delle mutazioni rimarrà esplorativa e descrittiva. Tutti i test saranno bilaterali con <math>\alpha = 0,05</math>, utilizzando R (v4.1.2).</p> |
| <p><b>TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 110-BIS DEL CODICE PRIVACY</b></p> | <p>Ai fini del presente studio, il trattamento dei dati personali è effettuato esclusivamente per finalità di ricerca scientifica, in conformità a quanto previsto dall'art. 110-bis del d.lgs. 196/2003 (Codice in materia di protezione dei dati personali). Ai sensi di tale disposizione, non è richiesta l'acquisizione del consenso al trattamento dati da parte degli interessati.</p> <p>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.</p> <p>L'estratto della DPIA è pubblicato sul sito web del Promotore."</p>                                                                                                                                                                                                                                                                                                                                                                                        |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SICUREZZA/GESTIONE EVENTI<br/>AVVERSI</b>         | <b>NA</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>DOCUMENTO DI RIFERIMENTO<br/>PER LA SICUREZZA</b> | <b>NA</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>BIBLIOGRAFIA</b>                                  | <p>1. Colombo N, Sessa C, Bois AD, et al. ESMO-ESGO consensus conference recommendations on ovarian cancer: pathology and molecular biology, early and advanced stages, borderline tumours and recurrent disease. <i>Int J Gynecol Cancer</i>. 2019;29(4):728-760. Published 2019 May 7. doi:10.1136/ijgc-2019-000308</p> <p>2. Ledermann JA, Matias-Guiu X, Amant F, et al. ESGO-ESMO-ESP consensus conference recommendations on ovarian cancer: pathology and molecular biology and early, advanced and recurrent disease. <i>Ann Oncol</i>. 2024;35(3):248-266. doi:10.1016/j.annonc.2023.11.015</p> <p>3. Trimbos JB, Parmar M, Vergote I, et al. International Collaborative Ovarian Neoplasm trial 1 and Adjuvant ChemoTherapy In Ovarian Neoplasm trial: two parallel randomized phase III trials of adjuvant chemotherapy in patients with early-stage ovarian carcinoma. <i>J Natl Cancer Inst</i>. 2003;95(2):105-112.</p> <p>4. Kleppe M, van der Aa MA, Van Gorp T, Slangen BF, Kruitwagen RF. The impact of lymph node dissection and adjuvant chemotherapy on survival: A nationwide cohort study of patients with clinical early-stage ovarian cancer. <i>Eur J Cancer</i>. 2016;66:83-90. doi:10.1016/j.ejca.2016.07.015</p> <p>5. Nero C, Bizzarri N, Di Berardino S, et al. Sentinel-node biopsy in apparent early stage ovarian cancer: final results of a prospective multicentre study (SELLY). <i>Eur J Cancer</i>. 2024;196:113435. doi:10.1016/j.ejca.2023.113435</p> <p>6. Ditto A, De Cecco L, Paolini B, et al. Validation of MiROvaR, a microRNA-based predictor of early relapse in early stage epithelial ovarian cancer as a new strategy to optimise patients' prognostic assessment. <i>Eur J Cancer</i>. 2022;161:55-63. doi:10.1016/j.ejca.2021.11.003</p> <p>7. Pesenti C, Beltrame L, Velle A, et al. Copy number alterations in stage I epithelial ovarian cancer highlight three genomic patterns associated with prognosis. <i>Eur J Cancer</i>. 2022;171:85-95. doi:10.1016/j.ejca.2022.05.005</p> <p>8. Camarda F, Mastrantoni L, Parrillo C, et al. Actionable mutations in early-stage ovarian cancer according to the ESMO Scale for Clinical</p> |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>Actionability of molecular Targets (ESCAT): a descriptive analysis on a large prospective cohort. ESMO Open. 2025;10(1):104090. doi:10.1016/j.esmoop.2024.104090</p> <p>9. Tie J, Cohen JD, Lahouel K, et al. Circulating Tumor DNA Analysis Guiding Adjuvant Therapy in Stage II Colon Cancer. N Engl J Med. 2022;386(24):2261-2272. doi:10.1056/NEJMoa2200075</p> <p>10. Guo K, Lu J, Lou Y, Zheng S. Prognostic value of postoperative ctDNA detection in patients with early non-small cell lung cancer: a systematic review and meta-analysis. Ther Adv Med Oncol. 2023;15:17588359231177008. Published 2023 May 27. doi:10.1177/17588359231177008</p> <p>11. Taliento C, Morciano G, Nero C, et al. Circulating tumor DNA as a biomarker for predicting progression-free survival and overall survival in patients with epithelial ovarian cancer: a systematic review and meta-analysis. Int J Gynecol Cancer. 2024;34(6):906-918. Published 2024 Jun 3. doi:10.1136/ijgc-2024-005313</p> <p>12. Hou JY, Chapman JS, Kalashnikova E, et al. Circulating tumor DNA monitoring for early recurrence detection in epithelial ovarian cancer. Gynecol Oncol. 2022;167(2):334-341. doi:10.1016/j.ygyno.2022.09.004</p> <p>13. Lo YMD, Han DSC, Jiang P, Chiu RWK. Epigenetics, fragmentomics, and topology of cell-free DNA in liquid biopsies. Science. 2021 Apr 9;372(6538):eaaw3616. doi:10.1126/science.aaw3616. PMID: 33833097.</p> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 2.3 TIPOLOGIA DI STUDIO

- Monocentrico
- No-profit<sup>1</sup>
- Retrospectivo

<sup>1</sup> 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).

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 2.4 NUMERO DI PAZIENTI ARRUOLATI

50 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) I dati raccolti dei partecipanti agli studi sono pseudonimizzati attraverso l'utilizzo di un ID univoco generato automaticamente da REDCap, che non contiene alcuna informazione direttamente riconducibile al paziente.

Il collegamento tra l'ID REDCap e l'identità del paziente è possibile solo tramite il codice sanitario, che rappresenta l'identificativo univoco utilizzato all'interno del nostro istituto.

Tuttavia, il codice sanitario, pur essendo tecnicamente un dato identificativo, non consente l'identificazione diretta da parte di soggetti esterni, in quanto può essere associato al paziente solo tramite l'accesso al sistema informativo clinico TrakCare, accesso che è riservato esclusivamente al personale autorizzato dell'ospedale e tramite connessione sicura, tracciata e controllata.

2) Qualora necessario e richiesto dal PI, è possibile raccogliere dati identificativi del paziente che vengono archiviati separatamente sia logicamente sia fisicamente dai dati clinici raccolti durante lo studio.

Tale separazione è gestita in modo automatizzato attraverso l'utilizzo di un modulo esterno sviluppato ad hoc da personale dedicato della Facility DC e integrato nella piattaforma REDCap (FPG Record Sensitive Data). Questo modulo consente, al momento dell'inserimento dei dati, di archiviare automaticamente eventuali dati identificativi che necessitano di essere raccolti in un database separato rispetto ai dati clinici, crittografati e accessibili solo ad utenti con particolari permessi/privilegi qui elencati:

- Selezione del Data Access Groups presente nella configurazione del modulo esterno
- Ruolo PI sempre abilitato

Questa configurazione è coerente con quanto previsto:

- dall'art. 89 del GDPR, che consente il trattamento di dati particolari per finalità di ricerca scientifica, subordinandolo all'adozione di misure tecniche e organizzative adeguate;
- dalle ICH-GCP, che richiedono che l'identità dei soggetti non sia direttamente accessibile al promotore o a terzi non autorizzati;
- dalle linee guida del Garante per la protezione dei dati personali e dalle indicazioni dell'AIFA –Ufficio Ispezioni GCP, che ribadiscono la necessità di limitare la diffusione dei dati identificativi, garantire la tracciabilità dei trattamenti e implementare misure di sicurezza quali:
  - la separazione logica e fisica dei dati;
  - la pseudonimizzazione;
  - il controllo degli accessi;



## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- la cifratura dei dati
- la valutazione d'impatto (DPIA) nei casi previsti;
- e la formazione del personale coinvolto.
- I dati che il modulo gestisce al momento sono i seguenti:

- Nome
- Cognome
- Data di nascita
- Email
- Numero di telefono

Quando l'utente, che ha i permessi/privilegi necessari, si trova ad aggiungere un nuovo record sulla eCRF, o quando si trova sul primo "instrument" della stessa, qualora non siano già stati inseriti i dati sensibili, si visualizza tramite un pop-up una maschera che permette di inserire le informazioni sopra citate.

Il modulo crea anche un pulsante sulla eCRF che consente, all'utente con i permessi/privilegi, di visualizzare i dati inseriti precedentemente.

Una volta salvati i dati tramite la maschera, vengono codificati con la crittografia: AES-128-CTR e con una chiave preimpostata, successivamente vengono caricati all'interno di un database dedicato, dove è presente una tabella per la loro archiviazione.

In questo modo i dati non sono più in chiaro e possono essere visualizzati solo attraverso la decodifica con la chiave preimpostata ed esclusivamente per gli utenti con i diritti sopra citati.

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

1) Nel caso di pseudoanonimizzazione, sia l'ID REDCap sia il codice sanitario del paziente sono registrati all'interno del database REDCap. Tuttavia, il collegamento tra il codice sanitario e l'identità del paziente è possibile solo tramite il sistema clinico TrakCare, accessibile esclusivamente da personale autorizzato dell'ospedale. Pertanto, la "tabella di conversione" tra dato pseudonimizzato e identità del paziente non è contenuta in REDCap, ma è implicita e custodita all'interno di TrakCare, garantendo la separazione logica tra i dati clinici e identificativi.

2) Nel caso di registrazione di dati sensibili (nome, cognome, data di nascita completa, email, numero di telefono) attraverso l'utilizzo del modulo FPG Record Sensitive Data la "tabella di conversione" è ospitata su un server diverso dal server che ospita il database dei dati clinici, i dati sensibili sono codificati con la crittografia: AES-128-CTR e con una chiave preimpostata e possono essere visualizzati solo attraverso la decodifica con la chiave preimpostata ed esclusivamente per gli utenti con i diritti sopra citati

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

I dati vengono inseriti manualmente in REDCap da personale dedicato e da una task force di clinici appositamente formata. Per garantire l'integrità del dato, vengono adottate le seguenti misure:  
Controlli incrociati tra fonti cliniche (es. cartella elettronica, referti) prima dell'inserimento.

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Validazioni automatiche in REDCap (es. range di valori, campi obbligatori, formati predefiniti).

Revisione periodica dei dati inseriti da parte di un supervisore o data manager.

Aggiornamenti effettuati solo da personale autorizzato, con tracciabilità delle modifiche tramite il sistema di audit trail di REDCap.

Queste procedure assicurano che i dati siano accurati, coerenti e aggiornati, in linea con i requisiti di qualità per gli studi clinici.

- **Il PI ha edotto il personale coinvolto nello studio sui comportamenti da tenere in caso di violazione, anche presunta, dei dati personali (data breach)? (specificare la modalità)**

Sì. Il Principal Investigator (PI) ha provveduto a istruire in modo esaustivo tutto il personale coinvolto nello studio in merito ai comportamenti da adottare in caso di violazione, anche presunta, dei dati personali (data breach). La formazione è stata erogata attraverso una sessione dedicata durante la Site Initiation Visit (SIV), integrata da un modulo formativo specifico sui principi del GDPR, sulle misure di sicurezza adottate nello studio e sulle modalità di segnalazione e gestione delle violazioni.

Durante il training sono stati illustrati:

Le definizioni di data breach (accesso non autorizzato, perdita, modifica, divulgazione o distruzione accidentale o illecita dei dati);

Le procedure da seguire in caso di sospetta violazione, inclusa la notifica immediata al PI e al Data Protection Officer (DPO) dell'istituto;

I tempi di notifica previsti dalla normativa (entro 72 ore dalla scoperta del data breach);

I canali ufficiali di comunicazione interna per la segnalazione;

Le responsabilità individuali e collettive in materia di protezione dei dati personali.

Infine, il PI ha previsto richiami periodici delle procedure di sicurezza durante le riunioni di avanzamento studio, per garantire il costante aggiornamento e la consapevolezza del team sul tema della sicurezza dei dati.

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 2.6 DATABASE E SOFTWARE UTILIZZATI

- Indicare i database aziendali utilizzati per raccogliere i dati da utilizzare per lo Studio (es: PACS, TrakCare, etc)

Trakcare

- Per lo studio è necessario utilizzare il/i software/dispositivi/piattaforme online:

|   | Nome software/dispositivo/piattaforma | Funzione/utilizzo | Indicare se il Software è installato in FPG o in cloud | Indicare il Fornitore /o indicare se open source |
|---|---------------------------------------|-------------------|--------------------------------------------------------|--------------------------------------------------|
| 1 | RedCap                                | eCRF              | FPG                                                    | NA                                               |
| 2 | IBM-SPSS Statistical Software         | statistica        | FPG                                                    | IBM                                              |

Il software SPSS elabora 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 tale software.

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 2.7 CRF/ECRF

- In caso di eCRF indicare software/piattaforma utilizzata

#### **RedCap Research Electronic Data Capture**

Il software utilizzato per la raccolta e gestione dei dati è REDCap, una piattaforma sviluppata dalla Vanderbilt University e distribuita con licenza gratuita per scopi non commerciali. Nel nostro caso, REDCap è ospitato e gestito internamente dalla Fondazione, che ne cura l'installazione, la configurazione e la manutenzione. Pertanto, non si tratta di un servizio in outsourcing, ma di una piattaforma gestita direttamente dall'ente

- Indicare se il software/ piattaforma utilizzata è di proprietà di Fondazione o di un fornitore esterno (outsourcing) : **NA**
- In caso di outsourcing indicare fornitore della piattaforma **NA**
- Indicare modalità di scambio dei files provenienti dai centri di sperimentazione (caso multicentrico) **NA**
- 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

In caso di risposta affermativa compilare le tabelle seguenti:

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- Deposito campioni biologici presso biobanche **esterne**/biorepository /laboratori per analisi

|   | Nome laboratorio                     | Indirizzo |
|---|--------------------------------------|-----------|
| 1 | Guardant Health presso Palo Alto USA |           |

- Corrieri e trasportatori di materiale biologico, dataset contenuti in supporti fisici, etc

|   | Nome Fornitore          | Indirizzo |
|---|-------------------------|-----------|
| 1 | In corso di valutazione |           |
| 2 |                         |           |
| 3 |                         |           |
| 4 |                         |           |
| 5 |                         |           |

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

Tutti i soggetti che tratteranno i dati personali sono stati nominati come da Istruzione Operativa - IO.018

☒ SI

☐ NO

### 2.10 RUOLI PRIVACY

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

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

|  | Autonomi titolari | Indirizzo |
|--|-------------------|-----------|
|  | \                 |           |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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

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

|   | Nome Fornitore          | Indirizzo |
|---|-------------------------|-----------|
| 1 | In corso di valutazione |           |

- Fornitori/gestori/manutentori di applicativi/software outsourcing (es. eCRF, Diario elettronico, APP di monitoraggio, APP/Software collegabili a dispositivi indossabili connessi, tele visita/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/laboratori esterni per analisi**  
☒ SI ☐ NO

|   | Nome laboratorio                     | Indirizzo | Ruolo Privacy                                   |
|---|--------------------------------------|-----------|-------------------------------------------------|
| 1 | Guardant Health presso Palo Alto USA |           | Responsabile esterno-contratto provvisto di SCC |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 2.11 TRASFERIMENTI DATI EXTRA UE

I dati sono trasferiti extra UE

☒ SI ☐ NO

USA: Guardant Health - PaloAlto

## 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)

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- 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;

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- 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,

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

n. 200 (Attuazione della direttiva 2005/28/CE recante principi e linee guida dettagliate per la buona pratica clinica relativa ai medicinali in fase di sperimentazione a uso umano).

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|-------------|-----------|--------------|---------|---------------|
|             | X         |              |         |               |

### 3.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

#### 3.21 Come sono informati del trattamento gli interessati?

Gli interessati sono informati tramite Informativa compilata a cura del Titolare (art. 13 GDPR) e pubblicata sul sito aziendale nella sezione del sito: <https://www.policlinicogemelli.it/servizi-paziente/privacy-e-protezione-dei-dati-personali/>.

| Valutazione | Accettata | Migliorabile | Critico | Non accettata |
|-------------|-----------|--------------|---------|---------------|
|             | X         |              |         |               |

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

Non applicabile. La presente DPIA consente di derogare all'acquisizione del consenso ai sensi dell'art 110 bis D.lgs. 30 giugno 2003, n. 196 come novellato dall'art. 44 comma 1 bis della legge 29 aprile 2024, n. 56 e come meglio specificato nelle FAQ (*Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca*) pubblicate dal GPDP e di seguito riportate:

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

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

| 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         |              |         |               |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 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  $Ri - (Ri \times \% \text{ di mitigazione})$ .

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.

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Il **rischio inerente** è il rischio che grava su un'organizzazione in assenza di qualsiasi azione o misura in grado di ridurre 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  $G \times P$  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  $RI - RI \times \% \text{Mitigazione}$ .

### 5. ANALISI DEI RISCHI

#### 5.1 Tabella delle Contromisure tecniche

| ID | Misure |
|----|--------|
|----|--------|

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | <p>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:</p> <ul style="list-style-type: none"> <li>• Misure di pseudonimizzazione e crittografia dei dati personali</li> <li>• 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</li> <li>• 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</li> <li>• 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</li> <li>• 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</li> <li>• Misure per la protezione dei dati durante la trasmissione: ex VPN, Autenticazione a più fattori</li> <li>• Misure per la protezione dei dati durante l'archiviazione: ex Crittografia, Backup</li> <li>• 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.</li> <li>• 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;</li> <li>• Misure per garantire una conservazione limitata dei dati.</li> </ul> |
| 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 |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

|   |                                                                                                                                                                                  |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.<br>Il corso erogato al personale di FPG si basa sulla normativa vigente sul trattamento dei dati personali delle persone fisiche, ovvero, il Regolamento Europeo (UE) 2016/679 e il Codice in materia di protezione dei dati personali (D.Lgs. n. 196 del 2003) modificato e integrato dal D.Lgs. 101/2018.<br>Sono, inoltre, previsti degli specifici eventi formativi, in relazione agli specifici settori di competenza.<br>Sono altresì previste delle apposite indicazioni e linee guida specifiche per gli Studi Clinici. |
| 3  | Gov e PRO                                                                                | Vedi par. 3.13 della presente DPIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 4  | Gestione data breach                                                                     | Lo staff coinvolto nello studio è formato in merito alla pro. da adottare al verificarsi di un data breach.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 5  | E' presente un apposito spazio aziendale dove pubblicare informativa e DPIA dello studio | Vedi par. 3.22 della presente DPIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 5.4 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

|                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Riservatezza – accesso illegittimo ai dati</b>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere: <ul style="list-style-type: none"> <li>• Perdita di riservatezza dei dati personali protetti da segreto professionale;</li> <li>• Conoscenza da parte di terzi non autorizzati di dati particolari laddove si riesca a re-identificare l'interessato;</li> <li>• rischio di re-identificazione degli interessati/pazienti arruolati per i progetti di ricerca.</li> </ul> |
| <b>Integrità – modifica indesiderata dei dati</b>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere: <ul style="list-style-type: none"> <li>• Perdita del controllo della qualità del dato.</li> <li>• Inoltre, nel caso di modifica indesiderata dei dati, la Fondazione potrebbe incorrere nel rischio di veder vanificate le attività di ricerca.</li> </ul>                                                                                                                |
| <b>Disponibilità – perdita dei dati</b>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere: <ul style="list-style-type: none"> <li>• Nessuno sull'interessato, trattandosi di dati copiati dai DB aziendali ai software di ricerca e non utilizzati a fini di cura ma di ricerca.</li> </ul>                                                                                                                                                                          |

### 5.5 Quali sono le principali minacce che potrebbero concretizzare il rischio?

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Riservatezza – accesso illegittimo ai dati</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 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). |
| <b>Integrità – modifica indesiderata dei dati</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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.

## DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

### 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.

Approvata dal DPO il 23/02/2025

Avv. Francesco Giorgianni

### 8. DOCUMENTI A SUPPORTO

omissis