

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

DATA PROTECTION IMPACT ASSESSMENT STUDI CLINICI

ESTRATTO

ID DELLO STUDIO: 7443

NOME DELLO STUDIO: RU-LACC

PRINCIPAL INVESTIGATOR: PROFESSORESSA ANTONIA CARLA TESTA

24/03/2026

Sommario

1. CONSIDERAZIONI PRELIMINARI	4
2. DESCRIZIONE DELLO STUDIO - Contesto, responsabilità, standard, risorse di supporto	5
2.1 Specificare ID e Titolo originale dello Studio.....	5
2.2 Sinossi dello Studio.....	5
2.3 Tipologia Di Studio	9
2.4 Numero Di Pazienti Arruolati.....	9
2.5 Dataset, Pseudonimizzazione, controlli di integrità, Data breach.....	9
2.6 Database E Software Utilizzati	11
2.7 CRF/eCRF	12
2.8 Campioni Biologici.....	12
2.9 Risorse: Soggetti interni coinvolti nello studio (ruoli e funzioni).....	13
2.10 Ruoli Privacy.....	13

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

2.11	Trasferimenti dati extra UE.....	14
3.	PRINCIPI FONDAMENTALI	15
3.1	PROPORZIONALITÀ E NECESSITÀ	15
3.11	Gli scopi del trattamento sono specifici, espliciti e legittimi?	15
3.12	Quali sono le basi legali che rendono lecito il trattamento?	15
3.13	Ci sono standard applicabili al trattamento?	15
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)?	17
3.15	I dati sono esatti e aggiornati?	17
3.16	Qual è il periodo di conservazione dei dati?	17
3.2	MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI.....	18
3.21	Come sono informati del trattamento gli interessati?	18
3.22	Ove applicabile: come si ottiene il consenso degli interessati?	18
3.23	Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?	18
3.24	Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	19
3.25	Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	19
3.26	Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	19
3.27	In caso di trasferimento di dati al di fuori dell'unione europea, i dati godono di una protezione equivalente?.....	20
4.	CALCOLO DEL RISCHIO	20
5.	ANALISI DEI RISCHI	21
5.1	Tabella delle Contromisure tecniche	21
5.2	Tabella delle Contromisure logistiche	22
5.3	Tabella delle Contromisure Organizzative	22

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO



5.4 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?..... 23

5.5 Quali sono le principali minacce che potrebbero concretizzare il rischio? 24

5.6 Quali sono le fonti di rischio? 25

5.7 Quali misure fra quelle individuate contribuiscono a mitigare il rischio? 25

6. RISULTATI DPIA E AZIONI DI MIGLIORAMENTO25

7. RISULTATI DPIA – PARERE DEL DPO.....26

8. DOCUMENTI A SUPPORTO26

ATTIVITA'	FUNZIONE	RESPONSABILE	DATA
Redatto da:	Ufficio Privacy	\	24/03/2026
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 2024 *“FAQ - Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca”* a seguito delle modifiche al Codice Privacy introdotte nell’art. 44 comma 1 bis della legge 29 aprile 2024, n. 56.

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

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

L’art. 110-bis, comma 4 del Codice costituisce una di quelle disposizioni di legge, che si inseriscono nello spazio di normazione lasciato agli Stati membri, ai sensi dell’art. 9, par. 2, lett. j) del Regolamento, alle quali fa riferimento l’art. 110 (primo comma, primo periodo) del Codice nella parte in cui prevede che: “1. Il consenso dell’interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell’Unione europea in conformità all’articolo 9, paragrafo 2, lettera j), del Regolamento, [...] ed è condotta e resa pubblica una valutazione d’impatto ai sensi degli articoli 35 e 36 del Regolamento”.

Nelle medesime FAQ il 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

ID 7443 - Ruolo della Radiomica applicata all'Ecografia in pazienti con Carcinoma della cervice localmente avanzato: uno studio retrospettivo multicentrico (Studio RU-LACC).

2.2 SINOSI DELLO STUDIO

Titolo	Ruolo della Radiomica applicata all'Ecografia in pazienti con Carcinoma della cervice localmente avanzato: uno studio retrospettivo multicentrico (Studio RU-LACC).
Background	<p>Il carcinoma cervicale è il quarto tumore più comune tra le donne a livello mondiale [1]. Nonostante il calo dell'incidenza, grazie agli screening per il papillomavirus umano (HPV) e alle campagne di vaccinazione, nel 2020 sono stati stimati 604.127 casi di carcinoma cervicale e 341.831 decessi [2]. Attualmente, la chirurgia è lo standard di trattamento per il carcinoma cervicale in stadio iniziale (stadio FIGO 2018 IA1-IIA1, escluso IB3), mentre per i pazienti con carcinoma cervicale localmente avanzato (LACC; stadio FIGO 2018 IB3-IVA, escluso IIA1) lo standard è la chemioradioterapia esclusiva (E-RTCT) [3, 4]. La chemioradioterapia neoadiuvante seguita da chirurgia radicale è ancora oggetto di dibattito, ma talvolta considerata [5, 6]. Un vantaggio della chirurgia post-trattamento neoadiuvante è la possibilità di valutare il residuo tumorale tramite istologia, correlato fortemente alla sopravvivenza [7].</p> <p>Secondo le linee guida europee, l'ecografia transvaginale/transrettale eseguita da un esperto o la Risonanza Magnetica (RM) sono obbligatorie per la valutazione primaria nella stadiazione locale del carcinoma cervicale [4], mostrando risultati comparabili nella rilevazione del tumore e della sua estensione locale [8] e una simile accuratezza nella rilevazione delle macrometastasi nei linfonodi sentinella [9]. Inoltre, l'ecografia offre molti</p>

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

	<p>vantaggi rispetto alla RM, come la convenienza economica, la maggiore disponibilità e la non invasività.</p> <p>La radiomica è un campo di ricerca in rapido sviluppo basato sull'estrazione di caratteristiche quantitative dalle immagini radiologiche, che vengono utilizzate insieme ai dati clinici per costruire modelli statistici di supporto alla diagnosi e alla gestione personalizzata [10]. Queste caratteristiche forniscono informazioni biologiche uniche e sono correlate a diversi outcome, come la probabilità di recidiva, la risposta al trattamento o la sopravvivenza. [11]. Secondo una revisione sistematica [12], le caratteristiche radiomiche estratte da RM e PET/CT sembrano avere un ruolo predittivo nella sopravvivenza (sopravvivenza globale e sopravvivenza libera da malattia) e nella risposta al trattamento nei pazienti con LACC.</p> <p>In letteratura, solo cinque studi hanno esplorato il ruolo dell'intelligenza artificiale applicata all'ecografia nel carcinoma cervicale [13]; tra questi, Jin X et al. hanno analizzato, in una serie di 172 pazienti, la capacità dei metodi radiomici basati sull'ecografia di discriminare in modo non invasivo tra metastasi linfonodali positive e negative nel carcinoma cervicale iniziale, ottenendo un AUC di 0,77 nel set di validazione interno [14]. Tuttavia, non sono ancora disponibili studi pubblicati sul ruolo dei metodi radiomici basati sulle caratteristiche testurali delle immagini ecografiche del tumore primario nei pazienti con LACC.</p>
Razionale	L'obiettivo di questo studio è applicare l'analisi radiomica alle immagini ecografiche di pazienti con carcinoma cervicale localmente avanzato (LACC) per predire la risposta al trattamento e la recidiva della malattia.
Tipologia Studio	Questo è uno studio osservazionale retrospettivo multicentrico.
Obiettivo Primario	Identificare le caratteristiche radiomiche ecografiche che possono discriminare le pazienti con carcinoma della cervice localmente avanzato che rispondono al trattamento (E-RTCT o N-CTRT seguita da chirurgia) da quelle che non rispondono, e di sviluppare e validare modelli di machine learning basati sull' ecografia per differenziare le pazienti responder dalle <i>non responder</i> .

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Obiettivi secondari	Sviluppare e validare modelli di machine learning basati su ecografia che includono le <i>features radiomiche</i> , per discriminare le pazienti con LACC che recidivano (<i>Relapse group</i>) da quelle che non recidivano (<i>Non-relapse group</i>), con un follow-up minimo di 18 mesi dal trattamento primario.
Criteri inclusione	<ol style="list-style-type: none"> 1. Età >18 anni 2. Pazienti con LACC confermato istologicamente, secondo lo stadio FIGO 2018 (IB3-IVA, escluso IIA1) [3], trattati presso Fondazione Policlinico Universitario A. Gemelli, IRCCS; Charles University and General University Hospital in Prague o presso Department of Gynecologic Oncology, IRCCS National Cancer Institute, Milan, Italy. 3. Istotipi: squamoso, adenocarcinoma e adenosquamoso 4. Pazienti sottoposti a esame ecografico prima del trattamento 5. Pazienti con almeno un'immagine ecografica DICOM del tumore solido 6. Pazienti trattati con chemioradioterapia esclusiva o con chemioradioterapia neoadiuvante seguita da chirurgia radicale. 7. Pazienti con almeno 18 mesi di follow-up dal trattamento primario.
Criteri esclusione	<ol style="list-style-type: none"> 1. Età <18 anni 2. Pazienti con immagini solo stampate, oppure immagini DICOM in cui i margini esterni del tumore cervicale non erano ben visibili, o con indicatori (<i>calipers</i>) o testo che coprono il tumore.
Piano Statistico (dimensionamento del campione ed analisi dei dati)	Stimiamo di includere almeno 220 pazienti, di cui 155 responder e 65 non-responder. Per sviluppare un modello radiomico per predire la risposta al trattamento, la coorte di pazienti verrà suddivisa casualmente in set di addestramento e di validazione con un rapporto di 75:25, mantenendo la stessa proporzione di pazienti responder e non-responder. Adattando le regole usuali per l'analisi di regressione, dovrebbero essere considerati almeno 10 pazienti con l'evento di interesse per ogni caratteristica selezionata. Un campione di 50 pazienti non-

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

responder per il set di addestramento consentirà di considerare circa 5 caratteristiche, un numero appropriato di variabili per sviluppare un modello radiomico.

Analogamente, per il modello di previsione della recidiva, stimiamo di includere almeno 190 pazienti, di cui 118 nel gruppo senza recidiva (con un follow-up minimo di 18 mesi dall'ultimo trattamento primario, E-RTCT o N-RTCT) e 72 nel gruppo con recidiva. Per costruire questo modello radiomico, anche in questo caso, la coorte verrà suddivisa casualmente in set di addestramento e di validazione con un rapporto di 75:25, preservando la proporzione tra i gruppi con e senza recidiva.

I modelli radiomici basati su ecografia per predire la risposta al trattamento e la recidiva saranno costruiti utilizzando la regressione logistica con penalità, random forest e classificatore xgboost, ottimizzati mediante validazione incrociata a 3-fold sul set di addestramento e testati sul set di validazione separato. Le variabili utilizzate nella costruzione del modello saranno caratteristiche cliniche, ecografiche e/o radiomiche che risulteranno statisticamente significative tra i due gruppi (Test di Wilcoxon-Mann-Whitney/test del chi-quadro con correzione di Benjamini-Hochberg per confronti multipli) e valutate come non ridondanti in base al coefficiente di correlazione di Pearson. Inoltre, saranno valutati altri metodi di selezione delle caratteristiche: l'eliminazione ricorsiva delle caratteristiche (RFE) e mRMR (Minimum-Redundancy-Maximum-Relevance). Descriveremo la capacità discriminativa come area sotto la curva delle caratteristiche operative del ricevitore (AUC) e la performance di classificazione come punteggio F1, sensibilità e specificità. Queste metriche saranno calcolate impostando come cut-off l'indice di Youden. Utilizzeremo l'approssimazione normale per stimare l'intervallo di confidenza (IC) al 95% per tutte le metriche tranne l'AUC. Per stimare l'IC al 95% delle AUC utilizzeremo il bootstrapping. La calibrazione del modello sarà valutata tramite il grafico di calibrazione. L'analisi statistica e la modellazione saranno eseguite in RStudio (R versione 3.6) e Python 3.9.

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

2.3 TIPOLOGIA DI STUDIO

- Multicentrico
- No-profit¹
- Retrospetivo

2.4 NUMERO DI PAZIENTI ARRUOLATI

222 pazienti

2.5 DATASET, PSEUDONIMIZZAZIONE, CONTROLLI DI INTEGRITÀ, DATA BREACH

- **Riportare una riga di dataset (es. CRF):**

I dati raccolti nell'ambito del presente studio sono inseriti in un foglio di lavoro Microsoft Excel, appositamente predisposto per la ricerca. Il file è protetto da password, condivisa esclusivamente con il Principal Investigator (PI) dello studio e con il personale coinvolto, come indicato nel protocollo. Tale misura è finalizzata a garantire un adeguato livello di sicurezza e a limitare l'accesso ai soli soggetti autorizzati.

La struttura del file Excel prevede una serie di variabili codificate, finalizzate alla gestione pseudonimizzata delle informazioni dei pazienti. A titolo esemplificativo, la seguente stringa rappresenta l'intestazione del foglio di lavoro:

"| ID paziente | Data di nascita | max tumor diameter (US) | LNF (0=no; 1=pelvic; 2=paraortic; 3=pelvic+paraortic) | TIPO PZ (1=PRICE; 2=LARA4; 3=UCSC E-RTCT; 4=PRAGA; 5=INT) | TRATTAMENTO (0=RTCT NAD+; 1=RTCT esclusiva) | Età alla diagnosi | Menopausa (0=no; 1=sì) | Data diagnosi | Data chirurgia | Grading Istologia (1=G1; 2=G2; 3=G3) | FIGO 2018 (0=IB3; 1=IIA2; 2=IIB; 3=IIIA; 4=IIIB; 5=IIIC1; 6=IIIC2; 7=IVA) | Istologia (1=squamoso; 2=adenocarcinoma; 3=adenosquamoso) | Data ultimo trattamento primario | Risposta radio NAD+ (0=completa; 1=parziale/stabilità; 2=no) | Risposta radiologica E-CTRT (0=completa; 1=parziale; 2=no) | Risposta chirurgica (0=pR0; 1=pR1; 2=pR2; 3=PD) | Risposta totale (0=risposta completa; 1=parziale/no) | TP adiuvante post IC (0=no; 1=sì) | Data TP

¹ In caso di No-profit Non co-finanziato Multicentrico, si prega di sottomettere al Comitato Etico anche eventuali contratti tra le parti (es. Data Transfer Agreement).

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

adiuvante | Recidiva/PD | Data recidiva | Status (0=viva; 1=morta) | Ultimo follow-up | OS | PFS1 | PFS2 | Immagine ECO DICOM per radiomica (0=no; 1=si) | Note”

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

Le pazienti arruolate nello studio vengono registrate in un file Microsoft Excel dedicato. A ciascuna paziente viene associato manualmente un codice identificativo numerico progressivo (ID), attribuito in ordine crescente al momento dell’inserimento nel file. Tale codice costituisce l’unico riferimento utilizzato per collegare i dati clinici, ecografici e istologici relativi alla paziente.

Tutti i dati raccolti sono pertanto associati esclusivamente all’ID numerico, senza includere elementi direttamente identificativi. Le immagini ecografiche in formato DICOM vengono rinominate utilizzando lo stesso codice identificativo e archiviate in cartelle dedicate.

L’associazione tra il codice ID e l’identità reale delle pazienti è conservata in un file separato e protetto da password, accessibile unicamente al Principal Investigator e al personale sanitario coinvolto nello studio, come specificato nel protocollo (Co-investigators e Investigators).

Solo i casi correttamente pseudonimizzati e completi di tutta la documentazione saranno inclusi nelle analisi statistiche previste dal protocollo.

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

Sì, la tabella di conversione che associa i codici pseudonimi all’identità reale dei pazienti è conservata in un luogo separato e sicuro rispetto ai dati pseudonimizzati. In particolare, la tabella è archiviata in un file protetto da credenziali, accessibile solo al personale autorizzato, e non è memorizzata nello stesso sistema o cartella contenente i dati clinici, ecografici e istologici pseudonimizzati. Questa separazione garantisce la protezione dell’identità dei soggetti e il rispetto delle normative sulla privacy.

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

I controlli sull’esattezza e l’aggiornamento dei dati avvengono attraverso procedure standardizzate previste dal protocollo dello studio. I dati clinici, ecografici e istologici vengono raccolti da personale adeguatamente formato, e ogni informazione viene verificata manualmente per coerenza e completezza sia al momento della raccolta che prima dell’inserimento nel database.

- **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)**

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Il Principal Investigator ha informato tutto il personale coinvolto nello studio sulle procedure da seguire in caso di violazione, anche solo presunta, dei dati personali. L’istruzione è avvenuta durante la formazione iniziale sul protocollo di studio e sulle norme di protezione dei dati, attraverso una sessione informativa. In tale occasione sono state illustrate le modalità per riconoscere un possibile data breach, l’obbligo di segnalazione immediata al Principal Investigator e, tramite questi, al Responsabile della Protezione dei Dati o al referente privacy dell’Ente.

2.6 DATABASE E SOFTWARE UTILIZZATI

PACS, 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	PACS	Archiviazione immagini	FPG	Intersystems
2	TrakCare	Ricerca dati	FPG	FPG
3	Microsoft Excel	Raccolta dati	FPG	FPG
4	One Drive	Trasferimento immagini da altri centri partecipanti	FPG	FPG
5	Aliza Medical imaging	Visualizzazione e contornazione US	FPG	Open
6	Visual Studio Code	Editor utilizzato per creazione linguaggio di programmazione Python per elaborazione immagini	FPG	Open
7	MODDICOM	Contornazione immagini	FPG	open
8	RStudio	Analisi dati/immagini e modellistica	FPG	Open

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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

2.7 CRF/ECRF

- In caso di eCRF indicare software/piattaforma utilizzata: NA
- Indicare se il software/ piattaforma utilizzata è di proprietà di Fondazione o di un fornitore esterno (outsourcing) a utilizzata: NA
- In caso di outsourcing indicare fornitore della piattaforma: NA
- **Indicare modalità di scambio dei files provenienti dai centri di sperimentazione (caso multicentrico):** Trasferimento di immagini ecografiche anonimizzate tramite la piattaforma OneDrive aziendale della Fondazione, con accesso riservato al personale autorizzato coinvolto nello studio.
- 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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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
1	1 Dr.ssa Valentina Chiappa Fondazione IRCCS Istituto Nazionale Dei Tumori, Milan, Italy	1 Dr.ssa Valentina Chiappa Fondazione IRCCS Istituto Nazionale Dei Tumori, Milan, Italy
2	2 Prof.ssa Daniela Fischerova Charles University and General University Hospital in Prague	2 Prof.ssa Daniela Fischerova Charles University and General University Hospital in Prague

- **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	\	

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO



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

	Nome software/dispositivo	Fornitore	Indirizzo
1	\		

- Contract Research Organization (CRO) SI NO

Se sì, specificare Nome, indirizzo e PEC della CRO

- Deposito campioni biologici presso biobanche /biorepository SI NO

	Nome laboratorio	Indirizzo	Ruolo Privacy
1	\		

2.11 TRASFERIMENTI DATI EXTRA UE

I dati sono trasferiti extra UE

- SI NO

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

3. PRINCIPI FONDAMENTALI

3.1 PROPORZIONALITÀ E NECESSITÀ

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

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

Norma di legge Art. 110 bis D.lgs n. 196/2003 e ss. mm. ii (Codice Privacy) in conformità degli articoli 9 lett J e 89 GDPR.

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

3.13 Ci sono standard applicabili al trattamento?

Gov e PRO

- REG:016 Rev:1.0 01/03/2024 (REGOLAMENTO RICERCA CLINICA)
- PRO.1049 PROCEDURA: Gestione delle Informative e dei Consensi Adempimenti in Materia di Protezione dei Dati Personali
- IO.018 Istruzione operativa: Data Privacy Manager, Data Privacy Manager Assistant e Incaricati Del Trattamento
- PRO.021: Procedura Gestione della Documentazione Sanitaria in Ospedale
- Nomine autorizzato al trattamento
- MAN 014: Manuale per l'Utilizzo per le Procedure Informatiche

La Ricerca Clinica è inoltre regolamentata dalla seguente normativa, da Standard Nazionali e Internazionali:

- Convenzione del Consiglio d'Europa per la protezione dei diritti dell'uomo e della dignità dell'essere umano (Convenzione di Oviedo del 04/04/1997, ratifica autorizzata con Legge 28/03/2001 n. 145);

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- Declaration of Helsinki (World Medical Association) “Ethical Principles for Medical Research Involving Human Subjects” del 1964 e ss.mm.ii;
- D.lgs 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali (recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) e ss.mm.ii.
- D.lgs 30 dicembre 1992, n. 502, recante riordino della disciplina in materia sanitaria, a norma dell’articolo 1 della legge 23 ottobre 1992, n. 421;
- D.M. Ministero della Salute 30 novembre 2021: Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52.
- D.M. Ministero della Salute 1° febbraio 2022: Individuazione dei comitati etici a valenza nazionale.
- d.M. Ministero della Salute 26 gennaio 2023: Individuazione di quaranta comitati etici territoriali.
- Linee guida di buona pratica clinica (Good Clinical Practice - GCP) e ss. mm.ii adottate dall’Unione Europea nel 1996, recepite nell’ordinamento italiano con D.M. 15 luglio 1997, n.162; ICH E6 (R3) GOOD CLINICAL PRACTICE GCP (luglio 2025)
- Linee guida “Per i trattamenti di dati personali del Garante per la Protezione dati personali nell'ambito delle sperimentazioni cliniche di medicinali” del 24 luglio 2008
- Regolamento (UE) n. 536/2014 del Parlamento Europeo e del consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE;
- Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR) che abroga la direttiva 95/46/CE;
- Regolamento (UE) n 2017/745 del Parlamento Europeo e del Consiglio del 5 aprile 2017 relativo ai dispositivi medici;
- Regolamento (UE) n 2017/746 del Parlamento Europeo relativo ai dispositivi medico diagnostici in vitro;
- Autorizzazione Generale del 22/2/2017 e ss modifiche (Autorizzazione Generale al trattamento di dati genetici);

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

3.14 I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Il trattamento avviene nel rispetto del principio di minimizzazione in quanto sono raccolti e trattati solo i dati strettamente necessari per il raggiungimento delle finalità dello Studio, come indicato nel Protocollo approvato dal Comitato Etico.

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

3.15 I dati sono esatti e aggiornati?

Il trattamento dei dati personali avviene in conformità del Protocollo dello Studio approvato dal Comitato Etico e nel rispetto dei principi di buona pratica clinica (GCP) a garanzia dell'esattezza dei dati raccolti e della non alterazione dei dati stessi; i dati sono costantemente aggiornati e fedelmente riportati nelle Schede Raccolta Dati cartacee (Case Report Forms –CRF) o elettroniche (electronics Case Report Forms- eCRF). Tutti i documenti essenziali sono raccolti nel Trial Master File (TMF) che è il fascicolo permanente della sperimentazione che consente di verificare in ogni momento come essa viene condotta e la qualità dei dati ottenuti. L'accesso ai dati necessari per lo studio è consentito solo al personale espressamente autorizzato che opera sotto la vigilanza del Medico Sperimentatore (Principal Investigator –PI); ogni accesso alle eCRF e al TMF è tracciato.

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

3.16 Qual è il periodo di conservazione dei dati?

I dati e i campioni biologici sono conservati per un arco di tempo non superiore a quello necessario per conseguire le finalità per le quali sono stati raccolti e trattati (art. 11, comma 1, lett. e) del Codice Privacy, il termine massimo di conservazione è di 7 anni dal termine dello studio, come da Provvedimento Autorità Garante del 18 luglio 2023 [9920977] "Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali - 24 luglio 2008 " che ha ritenuto congruo il termine di 7 anni desunto dall'art. 18 del D. Lgs. 6 novembre 2007, n. 200 (Attuazione della direttiva 2005/28/CE recante principi e linee guida dettagliate per la buona pratica clinica relativa ai medicinali in fase di sperimentazione a uso umano).

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

3.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

3.21 Come sono informati del trattamento gli interessati?

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

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

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

Nella informativa pubblicata sul sito sono fornite agli interessati specifiche indicazioni per esercitare il diritto di accesso e gli altri diritti riconosciuti dal GDPR, con indicazione dei dati di contatto del Titolare e del DPO aziendale.

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

L'esercizio dei diritti degli interessati può essere suscettibile di limitazioni in considerazione della finalità di ricerca scientifica nei limiti ed alle condizioni indicate dall'art. 89 GDPR. Il diritto alla portabilità dei dati non è applicabile in questo caso poiché la base giuridica del trattamento è una norma di legge (110 bis) e non è basato sul consenso dell'interessato (art. 20 GDPR).

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

L'interessato ha il diritto di chiedere al Titolare del trattamento la rettifica e la cancellazione dei dati con le modalità indicate nell'informativa scrivendo ai dati di contatto del Titolare e del DPO aziendale indicati nella stessa. Il diritto alla cancellazione può subire delle limitazioni per la finalità di ricerca scientifica in conformità di quanto previsto dall'art. 17, par. 3 lett. d) GDPR.

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

Nella informativa pubblicata sul sito sono fornite agli interessati specifiche indicazioni per esercitare i diritti riconosciuti dal GDPR, con indicazione dei dati di contatto del Titolare e del DPO aziendale. L'esercizio dei diritti degli interessati può essere suscettibile di limitazioni in considerazione della finalità di ricerca scientifica nei limiti ed alle condizioni indicate dall'art. 89 GDPR.

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

Gli obblighi dei responsabili del trattamento sono espressamente definiti nell'atto di nomina ex art. 28 GDPR ed anche contrattualizzati con apposito documento nei casi in cui i fornitori vengano a contatto (anche solo potenzialmente) coi dati personali a titolarità della Fondazione (ad esempio: laboratori di analisi esterni, corrieri esterni, fornitori di software provvisti di contratto di manutenzione, etc).

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO



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.

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): $RI = P \times G$.

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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

DPIA, Numero interessati, Data Breach. Ogni elemento presenta quattro scenari diversi ai quali è associato uno score da 1 a 4.

In base alla compilazione della tabella contenente gli elementi succitati si otterrà un punteggio di scoring compreso in un range da 9 a 36.

Associato allo scoring c'è il livello di Probabilità P (Improbabile, Poco Probabile, Probabile, Molto Probabile) col relativo punteggio di P (1-improbabile, 2-poco probabile, 3-probabile, 4-molto probabile).

La gravità o impatto rappresenta l'entità del danno in cui potrebbero incorrere gli interessati in quanto persone fisiche al manifestarsi di un rischio legato ad un data breach: tale danno può essere di natura fisica, materiale o immateriale, come da tabella sottostante. Il data breach può concretizzarsi a seguito di una perdita di Riservatezza (R), Integrità (I) e Disponibilità (D) del dato personale.

La stima della gravità di un accadimento avverso avviene attraverso la valutazione dei possibili danni divisi in tre categorie: Fisico (danni fisici subiti dall'interessato), Materiale (danni che coinvolgono le proprietà dell'interessato), Immateriale.

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

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

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

Il Rischio Residuo finale si calcola come $RI - RI \times \%Mitigazione$.

5. ANALISI DEI RISCHI

5.1 Tabella delle Contromisure tecniche

ID	Misure
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"> • Misure di pseudonimizzazione e crittografia dei dati personali • Misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di elaborazione, ad ex: firewall perimetrali, proxy, antivirus/antimalware sulle pdl e sui server, blocco delle installazioni sulle pdl, disattivazione automatica schermo, hardening dei sistemi, etc • Misure per garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico; ex backup e procedure di continuità operativa

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

	<ul style="list-style-type: none"> • Procedure per testare, valutare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento: ex effettuazione di VA periodiche • Misure per l'identificazione, l'autorizzazione e la profilazione degli utenti: ex: utenze AD, password policy, eliminazione account inattivi, accesso profilato ai software solo dietro autorizzazione, etc • Misure per la protezione dei dati durante la trasmissione: ex VPN, Autenticazione a più fattori • Misure per la protezione dei dati durante l'archiviazione: ex Crittografia, Backup • Misure per garantire la sicurezza fisica dei luoghi in cui vengono trattati i dati personali: ex badge elettronici di accesso consentono l'accesso agli ingressi comuni dell'edificio. La sicurezza degli ingressi comuni dell'edificio è garantita e gestita dai responsabili dell'edificio e dalle società di vigilanza; l'accesso ai sistemi IT (sala server e sala di archiviazione IT) è limitato al personale autorizzato con accesso tramite badge elettronico, come previsto da procedure specifiche. • Misure per garantire la configurazione del sistema, inclusa la configurazione predefinita: ex. disattivazione e/o modifica utenze di default su server e apparati di rete, gestione utenze di servizio automatizzate; • Misure per garantire una conservazione limitata dei dati.
2	I software/ Piattaforma fanno parte del Portafoglio Applicativo FPG
3	La tabella di conversione è conservata in un luogo/software separato rispetto al dato pseudonimizzato
4	I codici pseudonimizzati rispettano la previsione di non inserire riferimenti identificativi dei pazienti
5	Il trattamento dei dati personali avviene solo tramite dispositivi/ personal computer aziendali

5.2 Tabella delle Contromisure logistiche

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

5.3 Tabella delle Contromisure Organizzative

ID	Misure	Evidenze
1	Ruoli e responsabilità	Descritte nella IO 0.18 per i soggetti interni e descritte per lo studio in oggetto nei parr.2.7 e 2.8; i responsabili ex art 28 hanno

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

		<p>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).</p>
2	Formazione	<p>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.</p> <p>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.</p> <p>Sono, inoltre, previsti degli specifici eventi formativi, in relazione agli specifici settori di competenza.</p> <p>Sono altresì previste delle apposite indicazioni e linee guida specifiche per gli Studi Clinici.</p>
3	Gov e PRO	Vedi par. 3.13 della presente DPIA
4	Gestione data breach	Lo staff coinvolto nello studio è formato in merito alla pro. da adottare al verificarsi di un data breach.
5	E' presente un apposito spazio aziendale dove pubblicare informativa e DPIA dello studio	Vedi par. 3.22 della presente DPIA

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

<p>Riservatezza – accesso illegittimo ai dati</p> <p>Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere:</p> <ul style="list-style-type: none"> • Perdita di riservatezza dei dati personali protetti da segreto professionale; • Conoscenza da parte di terzi non autorizzati di dati particolari laddove si riesca a re-identificare l'interessato; • rischio di re-identificazione degli interessati/pazienti arruolati per i progetti di ricerca.

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO



<p>Integrità – modifica indesiderata dei dati</p> <p>Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere:</p> <ul style="list-style-type: none"> • Perdita del controllo della qualità del dato. • Inoltre, nel caso di modifica indesiderata dei dati, la Fondazione potrebbe incorrere nel rischio di veder vanificate le attività di ricerca.
<p>Disponibilità – perdita dei dati</p> <p>Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere:</p> <ul style="list-style-type: none"> • Nessuno sull'interessato, trattandosi di dati copiati dai DB aziendali ai software di ricerca e non utilizzati a fini di cura ma di ricerca.

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

<p>Riservatezza – accesso illegittimo ai dati</p> <p>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).</p>
<p>Integrità – modifica indesiderata dei dati</p> <p>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.</p>
<p>Disponibilità – perdita dei dati</p> <p>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.).</p>

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

5.6 Quali sono le fonti di rischio?

Riservatezza – accesso illegittimo ai dati
Fonti interne umane, fonti esterne non umane.
Integrità – modifica indesiderata dei dati
Fonti interne umane, fonti esterne non umane.
Disponibilità – perdita dei dati
Fonti interne umane, fonti esterne non umane.

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

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

6. RISULTATI DPIA E AZIONI DI MIGLIORAMENTO

Dall’analisi sulla gravità e le probabilità dei rischi emerge un valore di **Rischio Inerente** di livello **Moderato** (in una scala che prevede valori da lieve a moderato a grave a molto grave)

Nell’ottica di mitigazione di tali rischi si evince che, con l’implementazione delle misure tecnico/organizzative in atto, **il valore di abbattimento del Rischio Inerente, ovvero il Rischio Residuo, rientra in una condizione di accettabilità da parte dell’organizzazione.**

Al netto delle azioni di miglioramento si ritiene pertanto che **il trattamento in oggetto presenti un grado di rischio accettabile sui diritti e libertà dell’interessato** e di conseguenza non è richiesta una consultazione preventiva all’Autorità Garante.

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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

7. RISULTATI DPIA – PARERE DEL DPO

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

Approvato il /02/2026 dal DPO

Avv. Francesco Giorgianni

8. DOCUMENTI A SUPPORTO

omissis