



DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

DATA PROTECTION IMPACT ASSESSMENT STUDI CLINICI

ESTRATTO

ID DELLO STUDIO: 27005

NOME DELLO STUDIO: RIPARARE

PRINCIPAL INVESTIGATOR: DOTT. MARCELLO CANDELLI

11/03/2026

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	16
2.4 Numero Di Pazienti Arruolati.....	16
2.5 Dataset, Pseudonimizzazione, controlli di integrità, Data breach.....	16
2.6 Database E Software Utilizzati	21
2.7 CRF/eCRF	21
2.8 Campioni Biologici.....	22
2.9 Risorse: Soggetti interni coinvolti nello studio (ruoli e funzioni).....	22
2.10 Ruoli Privacy.....	22
2.11 Trasferimenti dati extra UE.....	24

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

3. PRINCIPI FONDAMENTALI	24
3.1 PROPORZIONALITÀ E NECESSITÀ	24
3.11 Gli scopi del trattamento sono specifici, espliciti e legittimi?	24
3.12 Quali sono le basi legali che rendono lecito il trattamento?	24
3.13 Ci sono standard applicabili al trattamento?	24
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)?	26
3.15 I dati sono esatti e aggiornati?	26
3.16 Qual è il periodo di conservazione dei dati?	26
3.2 MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI.....	27
3.21 Come sono informati del trattamento gli interessati?	27
3.22 Ove applicabile: come si ottiene il consenso degli interessati?	27
3.23 Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?	28
3.24 Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?	28
3.25 Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?	28
3.26 Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	29
3.27 In caso di trasferimento di dati al di fuori dell'unione europea, i dati godono di una protezione equivalente?.....	29
4. CALCOLO DEL RISCHIO	29
5. ANALISI DEI RISCHI	30
5.1 Tabella delle Contromisure tecniche	30
5.2 Tabella delle Contromisure logistiche	31
5.3 Tabella delle Contromisure Organizzative	32
5.4 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?.....	33

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

5.5	Quali sono le principali minacce che potrebbero concretizzare il rischio?	33
5.6	Quali sono le fonti di rischio?	34
5.7	Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	34
6.	RISULTATI DPIA E AZIONI DI MIGLIORAMENTO	35
7.	RISULTATI DPIA – PARERE DEL DPO.....	35
8.	DOCUMENTI A SUPPORTO	35

ATTIVITA'	FUNZIONE	RESPONSABILE	DATA
Redatto da:	Ufficio Privacy	\	09/03/2026
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 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

ID 27005

Ricerca di parametri clinico/laboratoristici e radiologici prognostici per le infezioni respiratorie acute e croniche riacutizzate delle basse vie aeree

2.2 SINOSSI DELLO STUDIO

TITOLO DELLO STUDIO

Ricerca di parametri clinico/laboratoristici e radiologici prognostici per le infezioni respiratorie acute e croniche riacutizzate delle basse vie aeree (RIPARARE)

PROMOTORE/SPONSOR

Fondazione Policlinico Universitario Agostino Gemelli IRCCS

CRO

N/A

(specificare anche attività delegate)

Cofinanziatore

N/A

(specificare se previsto scambio di informazioni di sicurezza)

SPERIMENTATORE PRINCIPALE

Dr. Marcello Candelli

BACKGROUND E RAZIONALE DELLO STUDIO

Le infezioni respiratorie acute rappresentano un importante fattore che induce la popolazione a recarsi in pronto soccorso visto il loro facile diffondersi nella popolazione dato l'alto tasso di contagiosità e di infezione soprattutto ma non solo nelle stagioni fredde. Possono essere classificate in infezioni della alte vie respiratorie quando coinvolgono le vie aeree superiori (cavità nasale e orale,

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

faringe laringe e trachea) e infezioni respiratorie delle basse vie aeree quando coinvolgono il bronchi e gli alveoli polmonari). I quadri maggiormente rappresentativi sono le bronchiti acute, le bronchiti croniche ostruttive riacutizzate e le polmoniti. L'etiologia è estremamente variabile. Le forme virali sono sostenute principalmente da virus influenzali, coronavirus (in particolare il SARS-CoV-2) e il virus respiratorio sinciziale mentre le forme batteriche più comuni sono date dallo S. pneumonie, dalla K. pneumonie e da batteri atipici (micoplasmi, clamidie e legionelle) e da numerosi altri batteri gram positivi e negativi. Più raramente invece e in genere nella popolazione immunodepressa possiamo avere forme micotiche (per esempio aspergillosi o pneumocistosi). In ogni caso le infezioni polmonari, soprattutto quando colpiscono pazienti anziani, immunodeficienti o comorbidi hanno una mortalità elevata. Per questo motivo molti pazienti con sindromi respiratorie si presentano nei pronto soccorsi aumentando il sovraffollamento. Rimane quindi fondamentale la ricerca di fattori prognostici che aiutino il medico di Pronto Soccorso ad eseguire una scelta in base a parametri oggettivi che possa facilitare l'invio in sicurezza verso il domicilio piuttosto che il ricovero ospedaliero (ed il setting a bassa, media o elevata intensità). In letteratura sono presenti alcuni score validati che hanno mostrato di essere utili ma che però non sono completamente esaustivi nel loro

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

compito. Con la comparsa nell'ultimo lustro dell'infezione da COVID19 sono stati presentati altri score che si sono dimostrati efficaci nel prevedere l'esito della patologie e la necessità del ricovero. Inoltre si è osservato come la vaccinazione per il l'influenza ha avuto un effetto protettivo aggiuntivo sull'esito del COVID19 con alla base probabilmente un meccanismo di rafforzamento incrociato immunitario.

OBIETTIVI DELLO STUDIO

Obiettivo primario dello studio è valutare, in un periodo di 5 anni, tra i pazienti con infezione delle basse vie respiratorie, la presenza di sintomi clinici, dati anamnestici, parametri laboratoristici e segni radiologici associati al quadro clinico, alla gravità della malattia e ai relativi esiti.

Obiettivi secondari:

- Valutare se gli score diagnostici già descritti in letteratura per il COVID19 (ancoc socre e 4c score) mantengono un'adeguata accuratezza prognostica anche nelle altre infezioni respiratore non legate al COVID19
- Valutare se i parametri statisticamente significativi individuati nell'obiettivo primario siano associabili in uno score predittivo per gli esiti studiati

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- Valutare se particolari parametri tra quelli studiati non ancora chiaramente associati all'esito di malattia (come vaccinazione antinfluenzale, anti COVID19 o anti pneumococcica siano associati alla prognosi delle infezioni della basse vie respiratorie
- Valutare differenze degli outcome in base allo stato vaccinale

ENDPOINT

Primari

- ospedalizzazione;
- ricovero in terapia intensiva;
- necessità di ventilazione;
- mortalità a 30 giorni.

Secondari

La performance degli score verrà analizzata attraverso:

- Analisi della *Receiver Operating Characteristic* (ROC) con calcolo dell'area sotto la curva (**AUC-ROC**) per ogni outcome valutato (mortalità a 30 giorni, necessità di ventilazione, ricovero in terapia intensiva, ospedalizzazione).
- Confronto statistico delle AUC (DeLong test).
- Calcolo dell'**Hosmer-Lemeshow test** o equivalenti più moderni (es. Spiegelhalter z-test) e Valutazione del Brier score per ciascun outcome.

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- *Decision Curve Analysis (DCA)* per quantificare il *net benefit* e valutare la rilevanza clinica degli score ai diversi threshold di rischio.
- Calcolo di sensibilità, specificità, VPP e VPN
- Testare le differenze di esito clinico tra pazienti vaccinati e non vaccinati.
- Costruzione e validazione di uno score predittivo per gli outcome clinici (mortalità, ventilazione, ICU, ospedalizzazione)

DISEGNO DELLO STUDIO OGGETTO DELLO STUDIO *Studio osservazionale retrospettivo senza farmaco e dispositivo monocentrico*

○

NUMERO DI PAZIENTI presso FPG e totali 2000

POPOLAZIONE TARGET *Paziente con infezioni respiratorie acute o croniche riacutizzate delle basse vie aeree che si sono presentati al Pronto Soccorso della Fondazione Policlinico Gemelli dal marzo 2020 al marzo 2025.*

CRITERI DI INCLUSIONE

- *età ≥ 18 anni*
- *Diagnosi di Infezione delle basse vie aeree confermata clinicamente e radiologicamente*

CRITERI DI ESCLUSIONE

- *Pazienti con infezione respiratoria e altra patologia acuta prevalente sulla prognosi del paziente (patologie che richiedono intervento chirurgico urgente, patologie tempo dipendenti, patologie acute con possibilità di esito infausto)*

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- *Pazienti minorenni*
- *Pazienti con patologie con prognosi inferiori a 1 mese*

TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 110 BIS DEL CODICE PRIVACY

Il Promotore ha provveduto a eseguire una Valutazione d'Impatto sulla protezione dei dati (DPIA), mediante la quale è stata accertata l'adeguatezza delle misure tecniche e organizzative adottate, al fine di garantire la tutela dei diritti e delle libertà fondamentali degli interessati, in conformità all'art. 89 del Regolamento (UE) 2016/679 e alle indicazioni del Garante per la protezione dei dati personali. Il trattamento dei dati sarà circoscritto alle finalità dello studio e condotto secondo i principi di minimizzazione, pseudonimizzazione e sicurezza, nel rispetto delle garanzie definite dall'Autorità Garante in materia. I dati saranno trattati con riservatezza e confidenzialità e divulgati solo in forma aggregata ed anonima, attendendosi a quanto raccomandato nella Convenzione di Oviedo e nella Dichiarazione di Helsinki. L'estratto della DPIA è pubblicato sul sito web del Promotore e dei centri di sperimentazione.

DURATA DELLO STUDIO e DURATA DELL'ARRUOLAMENTO

Due anni

TRATTAMENTO/PROCEDURA SPERIMENTALE

Per tutti i pazienti saranno raccolti i dati anagrafici, anamnestici, i parametri vitali e gli score prognostici classici (Scheda A), i sintomi (vedi scheda B), i dati laboratoristici eseguiti in PS (vedi scheda C) e dati delle indagini radiologiche (Scheda C). Andremo quindi a valutare gli esiti dei pazienti in termini di ospedalizzazione, ricovero in

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

terapia intensiva, necessità di ventilazione, morte a 30 giorni (questi dati saranno estratti dalle cartelle cliniche dei pazienti arruolati).

ANALISI STATISTICA e dimensionamento campionario

Dimensioni del campione

Assumendo un livello di significanza di 0,05, una potenza del 90% e un rapporto di rischio atteso di 1,18 (o 0,85), il numero minimo di eventi richiesti è stato stimato in 385. Basandosi su un tasso di eventi previsto di circa il 19% durante il periodo dello studio, sarà necessario un totale di circa 2000 pazienti arruolati consecutivamente per raggiungere questo numero di eventi, garantendo una potenza sufficiente per analisi multivariabili e valutazioni di sottogruppi.

Analisi statistica

Il software utilizzato per l'analisi statistica sarà IBM SPSS STATISTICS 16. Per l'analisi iniziale dei dati utilizzeremo una statistica descrittiva. I valori di numerosità saranno espressi come % del totale, i valori continui come media +/- deviazione standard (DS). I sintomi clinici, i dati di laboratorio e i risultati degli esami radiologici tra i vari gruppi saranno confrontati con un test Chi square o con uno student t test, ove appropriato. Sarà eseguita un'analisi multivariata sui fattori che all'analisi univariata avessero

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

presentato una significatività con $p < 0.01$ dopo correzione dei fattori confondenti come sesso, età e comorbidità. Una $p < 0.05$ sarà considerata significativa. I fattori che all'analisi multivariata resteranno significativamente correlati alla diagnosi di infezione o alla severità di malattia saranno inseriti rispettivamente in uno score prognostico di cui saranno calcolati sensibilità, specificità, VPP e VPN e il migliore cut off tramite la costruzione di una ROC. L'accuratezza diagnostica sarà valutata con il calcolo dell'AUROC e gli score diagnostici saranno paragonati tra loro per mezzo del metodo di De Long. In particolare, la capacità discriminativa dei punteggi verrà analizzata mediante la costruzione delle curve Receiver Operating Characteristic (ROC) e il calcolo dell'Area Under the Curve (AUC-ROC) per ognuno degli outcome considerati: mortalità a 30 giorni, necessità di ventilazione, ricovero in terapia intensiva e ospedalizzazione. Le differenze tra le AUC dei diversi score saranno valutate tramite DeLong test, al fine di confrontarne in modo statistico l'accuratezza discriminativa.

La calibrazione dei modelli sarà esaminata attraverso l'Hosmer-Lemeshow test o, in alternativa, mediante indicatori più recenti come lo Spiegelhalter z-test. Per ciascun outcome verrà inoltre calcolato il Brier score, che fornisce una misura complessiva della precisione predittiva del modello.

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Per valutare la rilevanza clinica dei punteggi e il loro potenziale impatto decisionale nelle differenti soglie di rischio, sarà eseguita una **Decision Curve Analysis (DCA)**, con quantificazione del *net benefit* associato a ciascun modello predittivo. Le differenze negli esiti clinici tra pazienti vaccinati e non vaccinati sono state analizzate mediante test χ^2 o test di Fisher per variabili categoriche, e tramite test t di Student o test di Mann–Whitney per variabili continue, a seconda della distribuzione dei dati.

Sarà sviluppato uno score predittivo per ciascuno degli outcome considerati mediante regressione logistica multivariabile o algoritmi di apprendimento automatico, a seconda della struttura dei dati e del numero di predittori. La selezione delle variabili sarà effettuata tramite criteri clinici e/o metodi data-driven (es. LASSO). La validazione interna del modello sarà condotta tramite bootstrapping o k-fold cross-validation, mentre la performance sarà valutata in termini di discriminazione, calibrazione e beneficio clinico secondo le metodiche descritte sopra.

SICUREZZA/GESTIONE EVENTI AVVERSI	N/A
DOCUMENTO DI RIFERIMENTO PER LA	N/A
SICUREZZA	



DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

BIBLIOGRAFIA

- 1) Algin A, Özdemir S, Afacan MA, Yusufoglu K, Özkan A. Comparative analysis of APUA, APUA-RO₂, and CURB-65 scores for mortality risk in hospitalized pneumonia patients. *Am J Emerg Med*. 2025 Nov;97:136-139. doi: 10.1016/j.ajem.2025.07.054. Epub 2025 Jul 23. PMID: 40716241.
- 2) Candelli M, Pignataro G, Ferrigno M, Cicchinelli S, Torelli E, Gullì A, Sacco Fernandez M, Piccioni A, Ojetti V, Covino M, Gasbarrini A, Antonelli M, Franceschi F. Factors Associated with ICU Admission in Patients with COVID-19: The GOL2DS Score. *Medicina (Kaunas)*. 2021;57:1356.
- 3) Covino M, De Matteis G, Burzo ML, Russo A, Forte E, Carnicelli A, Piccioni A, Simeoni B, Gasbarrini A, Franceschi F, Sandroni C; GEMELLI AGAINST COVID-19 Group. Predicting In-Hospital Mortality in COVID-19 Older Patients with Specifically Developed Scores. *J Am Geriatr Soc*. 2021;69:37-43.
- 4) Candelli M, Pignataro G, Ferrigno M, Cicchinelli S, Torelli E, Gullì A, Sacco Fernandez M, Piccioni A, Ojetti V, Covino M, Gasbarrini A, Antonelli M, Franceschi F. A new simple score to predict mortality of COVID-19 in the Emergency Department. *Signa Vitae*. 2022; in press.
- 5) Preti C, Biza R, Novelli L, Ghirardi A, Conti C, Galimberti C, Della Bella L, Memaj I, Di Marco F,

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Cosentini R. Usefulness of CURB-65, pneumonia severity index and MULBSTA in predicting COVID-19 mortality. Monaldi Arch Chest Dis. 2022

- 6) *Knight SR, Ho A, Pius R, Buchan I, Carson G, Drake TM, Dunning J, Fairfield CJ, Gamble C, Green CA, Gupta R, Halpin S, Hardwick HE, Holden KA, Horby PW, Jackson C, Mclean KA, Merson L, Nguyen-Van-Tam JS, Norman L, Noursadeghi M, Olliaro PL, Pritchard MG, Russell CD, Shaw CA, Sheikh A, Solomon T, Sudlow C, Swann OV, Turtle LC, Openshaw PJ, Baillie JK, Semple MG, Docherty AB, Harrison EM; ISARIC4C investigators. Risk stratification of patients admitted to hospital with covid-19 using the ISARIC WHO Clinical Characterisation Protocol: development and validation of the 4C Mortality Score. BMJ. 2020;*
- 7) *Candelli M, Pignataro G, Torelli E, Gullì A, Nista EC, Petrucci M, Saviano A, Marchesini D, Covino M, Ojetto V, Antonelli M, Gasbarrini A, Franceschi F. Effect of influenza vaccine on COVID-19 mortality: a retrospective study. Intern Emerg Med. 2021;16:1849-1855.*

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

2.3 TIPOLOGIA DI STUDIO

- Monocentrico
- No-profit Non co-finanziato¹
- Retrospettivo

2.4 NUMERO DI PAZIENTI ARRUOLATI

2000 pazienti

2.5 DATASET, PSEUDONIMIZZAZIONE, CONTROLLI DI INTEGRITÀ, DATA BREACH

- Riportare una riga di dataset (es. CRF)

SCHEDA A

DATI ANAGRAFICI, PARAMETRI VITALI E SCORE PROGNOSTICI

ID paziente pseudonimizzato	
SESSO	
Eta'	
Data della diagnosi	
Frequenza cardiaca	
Frequenza respiratoria	
Pressione arteriosa sistolica	
Pressione arteriosa diastolica	

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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

SO2	
Temperatura	
BMI	
Terapia in atto	
Comorbidità	
Gruppo Sanguigno	
Vaccino pneumococcico	
Vaccino per COVID 19: Tipo e numero di dosi	
Vaccino antinfluenzale	
GCS	
Curb-65	
Pneumonia severity index	
4C score	
ANCOC score	

SCHEDA B SINTOMI CLINICI

Sintomo	Giorni dalla visita in PS
Artralgia/Artrite	
Ipertransaminasemia	
Astenia	
Linfoadenopatia/linfadenite	
Cefalea	
Mialgia	
Congiuntivite	
Nausea	
Diarrea	
Febbre	
Dispnea	
Tosse secca	
Tosse produttiva	
Dolori Addominali	
Rigor Nucalis	
Emorragie cutanee/mucose	
Sepsi/shock settico	
Esantema/Rash Cutaneo	
Sindrome di tipo influenzale	
Faringite/faringodinia	
Vomito	



DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

Disgeusia	_____
Dis/anosmia	_____
Rinorrea	_____
Anoressia	_____

Altro, specificare _____ |
 COMORBIDITA': DIABETE – IPERTENSIONE – CARDIOPATIA ISCHEMICA – ALTRO:.....
 TERAPIA:.....

 FUMO DI SIGARETTA: Sì – No se Sì numero di pacchetti al giorno:.....
 Se ex fumatore numero di pacchetti al giorno e data di interruzione dal fumo.....

CHEDA C

PARAMETRI DI LABORATORIO

VALORE

AZOTEMIA	
CREATININA	
SODIO	
POTASSIO	
ALT	
BILIRUBINA	
LDH	
CPK	
Piastrine	
Hb	
Leucociti	
Neutrofili (n. assoluto e %)	
Linfociti (n. assoluto e %)	
Di-dimero	
INR	
Fibrinogeno	
PCR	
PCT	
Vit D	
Eosinofili (n. assoluto e %)	
Troponina	
Nt-pro-BNP	
Tampone antigenico (COI)	

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

PaO2	
PaCO2	
Lattati	
pH	
SaO2	
PaO2/FiO2	
Esami colturale escreato	
Esame colturale sange	
Tampone faringeo per virus respiratori	
Sierologia per infezioni respiratore	
PCR su campione biologico per virus respiratori	

ESAMI RADIOLOGICI

Rx torace:	interessamento interstiziale	SI	NO
	Interessamento alveolare	SI	NO
	Addensamenti	SI	NO
	Broncogramma aereo	SI	NO
	Versamento pleurico	SI	NO

ALTRO

TC torace:	Aree a vetro smerigliato	SI	NO
	Interessamento interstiziale	SI	NO
Interessamento alveolare	SI	NO	
	Addensamenti	SI	NO
	Broncogramma aereo	SI	NO
	Versamento pleurico	SI	NO

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

Utilizzeremo il metodo di pseudonimizzazione tramite hashing. il nome e il cognome di ciascun paziente sarà sostituito con un codice alfanumerico di 10 caratteri.

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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

La tabella di conversine verrà conservata in un armadio chiuso a chiave (la chiave è a disposizione del solo principal investigator che a sua volta si trova in una stanza in cui l'accesso è consentito esclusivamente tramite badge personale).

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

I dati vengono inseriti manualmente in foglio di microsoft EXCEL posto su PC della Fondazione su cui si accede esclusivamente con le credenziali dei ricercatori che prendono parte allo studio 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. Validazioni automatiche in Excel (es. range di valori massimo e minimo preimpostati, campi obbligatori, formati predefiniti). Revisione periodica dei dati inseriti da parte di un supervisore o data manager che controlla in particolare tutti i dati al di sopra o al di sotto del 95 percentile rispetto alla media. Aggiornamenti effettuati solo da personale autorizzato

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

L'eventualità che avvenga un data breach è stata discussa dal PI con tutto lo staff impegnato nel progetto di ricerca durante una riunione di preparazione dello studio, tenutasi in data 01-12-2025. In tale occasione, il PI ha illustrato le principali procedure irrinunciabili in caso di data breach. Il PI ha sottolineato l'importanza della tempestività della segnalazione al responsabile della Protezione dei Dati (DPO) e all'Autorità Competente, in conformità al Regolamento (UE) 2016/679 (GDPR) e alle policy interne dell'ente. La comunicazione è avvenuta in forma orale, durante la riunione sopra citata, alla presenza del personale coinvolto nello studio. Il PI ha inoltre previsto che tali aspetti relativi alla gestione di eventuali data breach verranno richiamati e approfonditi anche nel corso delle prossime riunioni e che ottenuta l'approvazione dello studio sarà inviata una mail a tutto il personale coinvolto per ribadire quanto detto in forma orale nella riunione del 25-11-2025. per garantire la costante condivisione e il rafforzamento della consapevolezza tra tutti i soggetti coinvolti.

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)

GIPSEweb, 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	R	statistica		Open source
2	Microsoft Excel	Raccolta dati	FPG	Microsoft

Il software R 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.

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)

Studio monocentrico

NA

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

- **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**

Le CRF saranno conservate in apposito armadio chiuso a chiave presso stanza della FPG a cui si accede solo tramite badge autorizzato dal direttore di UOC del PI. L'armadio ubicato nel reparto di medicina d'Urgenza si trova in un luogo diverso da quello in cui è conservata la tabella di conversione usata per la pseudonimizzazione.

2.8 CAMPIONI BIOLOGICI

- Campioni conservati nella biobanca di FPG e trattati in FPG

- ☐ SI
☒ NO

- Campioni inviati a biobanche o centri esterni per specifiche analisi

- ☐ SI
☒ NO

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

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

- ☒ SI
☐ NO

2.10 RUOLI PRIVACY

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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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

	Autonomi titolari	Indirizzo
1	\	
2		

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

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

	Nome Fornitore	Indirizzo
1	\	

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

	Nome software/dispositivo	Fornitore	Indirizzo
1	\		

- 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	\		

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

2.11 TRASFERIMENTI DATI EXTRA UE

I dati sono trasferiti extra UE

☐ SI ☒ NO

3. PRINCIPI FONDAMENTALI

3.1 PROPORZIONALITÀ E NECESSITÀ

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

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

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

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

Valutazione	Accettata	Migliorabile	Critico	Non accettata
	X			

3.13 Ci sono standard applicabili al trattamento?

Gov e PRO

- REG:016 Rev:1.0 01/03/2024 (REGOLAMENTO RICERCA CLINICA)

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): $RI = P \times G$.

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 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	I dati dello studio sono trattati tramite software installati su sistemi FPG e di conseguenza protetti dai sistemi e dalle policies di cybersecurity di FPG, che comprendono: • Misure di pseudonimizzazione e crittografia dei dati personali • Misure per garantire la riservatezza, l'integrità, la disponibilità e la resilienza costanti dei sistemi e dei servizi di elaborazione, ad ex: firewall perimetrali, proxy, antivirus/antimalware sulle pdl e sui server, blocco delle installazioni sulle pdl, disattivazione automatica schermo, hardening dei sistemi, etc • Misure per garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico; ex backup e procedure di continuità operativa • 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

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

DATA PROTECTION IMPACT ASSESSMENT MODELLO STUDI CLINICI - ESTRATTO

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

Riservatezza – accesso illegittimo ai dati
Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere: • Perdita di riservatezza dei dati personali protetti da segreto professionale; • Conoscenza da parte di terzi non autorizzati di dati particolari laddove si riesca a re-identificare l'interessato; • rischio di re-identificazione degli interessati/pazienti arruolati per i progetti di ricerca.
Integrità – modifica indesiderata dei dati
Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere: • Perdita del controllo della qualità del dato. • Inoltre, nel caso di modifica indesiderata dei dati, la Fondazione potrebbe incorrere nel rischio di veder vanificate le attività di ricerca.
Disponibilità – perdita dei dati
Con riferimento al Considerando 75 del GDPR i potenziali impatti potrebbero essere: • Nessuno sull'interessato, trattandosi di dati copiati dai DB aziendali ai software di ricerca e non utilizzati a fini di cura ma di ricerca.

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

Riservatezza – accesso illegittimo ai dati
Replica dei dati su supporto non sicuro/adatto, installazione di software non autorizzato sulla postazione di lavoro, divulgazione involontaria delle informazioni (es in un dialogo), attacco di ingegneria sociale per carpire informazioni/furto identità, mancata protezione dei pc (es. schermi non protetti), cambio mansione, dimissioni di dipendente, affidamento di attività di progetto/servizio a fornitori, infezioni da virus/malware, sistema di autenticazione/profilazione/gestione delle credenziali non adeguato, errori/vulnerabilità nel software utilizzato, trasmissioni di dati in maniera non sicura, comportamenti sleali o fraudolenti di dipendenti, furto di dispositivi (pc, telefono, HW).
Integrità – modifica indesiderata dei dati

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.

Approvato il /03/2026 dal DPO

Avv. Francesco Giorgianni

8. DOCUMENTI A SUPPORTO

omissis