**V1.0 data 14.05.2026**

# ESTRATTO della
# Valutazione di IMPATTO
# Studio "Profilo clinico e radiologico in MPO-ILD in confronto a fibrosi polmonare idiopatica (IPF)"

# "Clinical and radiological profile of MPO-ILD in comparison with pulmonary idiopathic fibrosis"
# codice MPOILDSTUDY

| | |
|---|---|
| Redatto: | vedasi sezione team di lavoro |
| Verificato: | DPO |
| Approvato: | Direttore Generale e Direttore Scientifico |
| Versione: | 1.0 |

**DATI DI CONTROLLO DEL DOCUMENTO**

| Storia del documento | | | | |
|---|---|---|---|---|
| versione | data | capitolo/paragrafo | modifica apportata | motivo modifica |
| 01 | 14.05.2026 | --- | Nessuna | Prima versione |

Sommario

# 1. Informazioni generali

## 1.1 Titolare del trattamento

La presente DPIA è stata redatta dalla Azienda Socio-Sanitaria Territoriale (ASST) di Mantova, in qualità di Titolare del trattamento ("Titolare del trattamento" o "ASST Mantova").
Tale ruolo è assunto in quanto la ASST è centro promotore e coordinatore dello studio dal titolo "P*rofilo clinico e radiologico in MPO-ILD in confronto a fibrosi polmonare idiopatica (IPF)*" codice dello studio "MPOILDSTUDY", avendone determinato il protocollo, versione n. 1.0 del 14/05/2026.
Il Principal Investigator (Responsabile dello studio) presso il promotore è il Dott. Enrico Colombo.
Co-Sperimentatori: Dr.ssa Jessica Gozzi, Dott. Paolo Francia.

## 1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti presso l'Ambulatorio di Reumatologia della Struttura complessa Allergologia, Immunologia Clinica e Reumatologia e presso l'Ambulatorio di Interstiziopatie della Struttura complessa Pneumologia della ASST Mantova, e presso gli ambulatori dei centri partecipanti, ai quali è stata diagnosticata una diagnosi di fibrosi polmonare idiopatica o interstiziopatia con anticorpi anti-MPO, reclutati per le finalità di ricerca al fine di condurre lo studio multicentrico, retrospettivo, osservazionale, dal titolo "P*rofilo clinico e radiologico in MPO-ILD in confronto a fibrosi polmonare idiopatica (IPF)*" codice dello studio "MPOILDSTUDY",

## 1.3 Standard di riferimento per la predisposizione della DPIA

La presente DPIA è stata realizzata utilizzando come base le informazioni contenute nel software sviluppato dall'Autorità francese per la protezione dei dati (CNIL), in conformità alle indicazioni fornite nelle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" (WP 248 rev. 01 e adottate dall'EDPB il 4 aprile 2017 e modificate il 4 ottobre 2017 – "***Linee Guida***").*
Inoltre, per la valutazione del rischio è stata utilizzata la metodologia dell'*European Union Agency For Network and Information Security* ("**ENISA**") descritta all'interno del documento "*Guidelines for SMEs on the security of personal data processing*" raggiungibile al seguente link https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data- processing.
Sono stati, infine, tenuti in considerazione alcuni dei requisiti della norma ISO/IEC 29134 "*Information technology — Security techniques — Guidelines for privacy impact assessment":* in particolare, valutazione necessità DPIA (art. 6.2), composizione del DPIA team (art. 6.3.1), piano di trattamento del rischio residuo e revisione e verifica della DPIA (art. 6.5.3 – 6.5.4).

## 1.4 Descrizione del quadro normativo e regolatorio, standard e buone prassi

- Regolamento UE 679/2016 [cons. 33-50-52-53-62-65-113-156-157-159-160-161-162-163; artt. 5-9-14-17-21-89];
- D.Lgs. 196/2003 (mod. D.Lgs. 101/2018) [artt. 78-100-105-106-110-110 *bis*]"), come modificato da ultimo dall'art. 1, comma 1, della l. 29 aprile 2024, n. 56. di conversione del D.L. 2 marzo 2024, n. 19;
- Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del

GDPR Versione 2.0 Adottate il 7 luglio 2021;
- Provvedimenti Autorità Garante [provv. GPDP 497/2018 riguardante le aut. gen. 9/2016 e aut. gen. 8/2016];
- GCP - ICH Harmonised Guideline – "Integrated Addendum to Ich E6(r1): Guideline For Good Clinical Practice", del 9 novembre 2016;
- EDPB – "Documento sulla risposta alla richiesta della Commissione europea di chiarimenti sull'applicazione coerente del GDPR, concentrandosi sulla ricerca sanitaria", adottato il 2 febbraio 2021;
- GPDP – Provvedimento del 9 maggio 2024, "Individuazione delle misure di garanzia ai sensi degli artt. 106, comma 2, lett. d) e 110 del Codice";
- Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Tecniques, April 2014;
- ISO/IEC 20889:2018 - Privacy enhancing data de-identification terminology and classification of techniques;
- ISO 25237:2017 – Health informatics – Pseudonymization;
- ISO/IEC 27559:2022 - Information security, cybersecurity and privacy protection – Privacy enhancing data de-identification framework;
- NIST - NISTIR 8053 De-Identification of Personal Information, October 2015;
- DICOM PS3:15 2016 – Annex E;
- NIST SP 800-188 De-Identifying Government Datasets: Techniques and Governance, September 2023;
- ENISA, "Data Pseudonymisation: Advanced Techniques & Use Cases Technical Analysis of Cybersecurity Measures iI Data Protection and Privacy", January 2021;
- ENISA, "Privacy Enhancing Technologies: Evolution and State of the Art", March 2017.
- nota interpretativa rilasciata dall'Autorità Garante per la protezione dei dati personali nelle FAQ dedicate alla ricerca scientifica del 6 giugno 2024;
- nota prot. n. G1.2024.0002222 del 22/01/2024 con cui Regione Lombardia, sulla scorta di quanto previsto dalla normativa comunitaria e dai citati decreti, chiarisce che il parere di un solo Comitato Etico Territoriale (CET) è valido per tutte le strutture lombarde coinvolte nello studio osservazionale;
- Determina AIFA n. 425 del 08/08/2024 avente per oggetto: "Linea Guida per la classificazione e conduzione degli studi osservazionali sui farmaci".

### 1.5 Procedura per la conduzione della DPIA

La presente DPIA si articola nelle seguenti fasi:

- Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA
- Fase 1: Descrizione del trattamento
- Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento
- Fase 3: Calcolo del rischio
- Fase 4: Misure di mitigazione del rischio adottate
- Fase 5: Consultazione degli interessati
- Fase 6: Calcolo del rischio residuo, piano di remediation e parere del DPO
- Fase 7: Consultazione dell'autorità garante per la protezione dei dati personali
- Fase 8: Monitoraggio e riesame nel tempo della DPIA ed eventuale aggiornamento

# 2. Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA

## 2.1 Necessità di svolgere la DPIA

Il Titolare del trattamento al fine di garantire che il trattamento dei dati relativi allo stato di salute dei pazienti arruolati nell'ambito dello studio sia svolto in conformità al Regolamento UE 2016/679 si impegna a rispettarne i principi fondamentali.

In particolare, si è provveduto a seguire i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati di cui al Regolamento (UE) 2016/679 (di seguito GDPR) così come schematizzati nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" del 4 ottobre 2017 pubblicate dal Gruppo di lavoro Articolo 29 (WP29), e si è riscontrato che i trattamenti presi in considerazione possono presentare rischi elevati.

> "ART. 35 Valutazione d'impatto sulla protezione dei dati. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi."

Il trattamento preso in esame, rispetto a quelli individuati nell'allegato 1 al provvedimento del Garante della protezione dei dati personali n. 467 dell'11 ottobre 2018, "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto", rientra nei:

- Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo) – (rif. 6);
- Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse – (rif. 10);

Preso atto che il sopracitato provvedimento asserisce che la valutazione d'impatto sulla protezione dei dati debba essere effettuata ogniqualvolta ricorra almeno un criterio in quanto è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati, si è ritenuto opportuno procedere all'esecuzione della valutazione d'impatto.

## 2.2 Team di lavoro

Il presente documento è stato redatto da un team composto da:

- Principal Investigator Struttura Allergologia Immunologia Clinica e Reumatologia
- Co-Investigator Strutture Pneumologia e Radiologia/diagnostica per Immagini
- Ufficio Affari Generali/privacy
- DPO (per le impostazioni metodologiche e per il parere sulla DPIA stessa).

## 2.3 Piano delle attività

Al termine della predisposizione della DPIA, il documento verrà sottoposto al parere del DPO.

# 3. Fase 1: Descrizione del trattamento

## 3.1 Il trattamento oggetto della Valutazione di Impatto

### 3.1.1 Il trattamento oggetto della Valutazione di Impatto

Si tratta di uno studio clinico Retrospettivo osservazionale, retrospettivo, su outcome, multicentrico, nazionale
Disegno: analitico di coorte.
I dati analizzati retrospettivamente riguarderanno i pazienti con età ≥ a 18 anni e diagnosi di fibrosi polmonare idiopatica o interstiziopatia con anticorpi anti-MPO afferiti nel periodo dal 2020 al 2025 all'ambulatorio di interstiziopatie della SC di Pneumologia o all'ambulatorio di Reumatologia della SC di Allergologia, Immunologia clinica e Reumatologia di Mantova, e agli ambulatori dei centri aderenti.
Il campione stimato è di circa 75 pazienti.

La mancata considerazione delle informazioni socio-demografiche e sanitarie riferite ai pazienti deceduti o non raggiungibili produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati compromettendo il conseguimento delle finalità della ricerca stessa. Per evitare un "bias" nella selezione dei pazienti e pregiudicare i risultati dello studio, i pazienti saranno considerati eleggibili indipendentemente dal loro stato attuale (in vita o deceduti) o dalla loro reperibilità.
Nel caso di specie, la malattia oggetto dello studio è caratterizzata da una elevata incidenza di mortalità. D'altra parte la raccolta dei dati di tutti i pazienti, inclusi quelli degli interessati deceduti è fondamentale per evitare potenziali bias di selezione nello studio.
Per evitare un "bias" nella selezione dei pazienti e pregiudicare i risultati dello studio, i pazienti saranno considerati eleggibili indipendentemente dal loro stato attuale (in vita o deceduti) o dalla loro reperibilità.

Lo studio osservazionale retrospettivo è basato su documentazione sanitaria già presente presso la ASST e i centri aderenti.
In particolare, saranno trattati in forma pseudonimizzata ed inseriti nella CRF i dati personali e particolari indicati nella scheda raccolta dati, e già raccolti in precedenza ai fini di cura della salute, presenti nei software aziendali (per ASST Mantova. Galileo, Dedalus, Firenze) e raccolti in un Data base Microsoft Excel, criptato, al quale potranno accedere solo gli sperimentatori coinvolti direttamente nello studio, e relativi a pazienti affetti da fibrosi polmonare idiopatica o da interstiziopatia con anticorpi anti-MPO, afferiti agli ambulatori di Pneumologia e Reumatologia della ASST Mantova e agli ambulatori dei centri partecipanti.
L'analisi retrospettiva dei dati riguarderà dati anagrafici (età, sesso, età alla diagnosi), clinici, laboratoristici e autoanticorpi, parametri spirometrici. Verranno estratti inoltre parametri radiologici mediante rilettura delle immagini HRCT eseguite alla diagnosi (t0) e dopo 24 mesi (t24) da parte di un solo radiologo toracico.

Gli obiettivi dello studio sono:

- Descrivere le caratteristiche cliniche, radiologiche e funzionali dell'interstiziopatia anti-MPO positiva (MPO-ILD);
- Individuare elementi clinici, radiologici e funzionali in grado di distinguere la MPO-ILD dalla IPF;
- Individuare eventuali predittori di sviluppo di vasculite nei pazienti affetti da MPO-ILD;

La durata dello studio è stimata in complessivi 12 mesi; 6 mesi dall'approvazione dello studio per la raccolta dati e 6 mesi per l'esecuzione delle analisi ed eventuale pubblicazione dei risultati.

I dati verranno estratti dalla documentazione sanitaria già presente (cartelle cliniche/applicativi aziendali) e raccolti in un database elettronico, criptato, al quale potranno accedere solo gli sperimentatori coinvolti direttamente nello studio.
I dati verranno trattati secondo quanto previsto dall'art. 89 GDPR, adottando adeguate garanzie per i diritti e le libertà dell'interessato attraverso la predisposizione di misure specifiche quali: tecniche di cifratura e pseudonimizzazione (codice alfanumerico per singolo paziente), che li rendono non direttamente riconducibili all'interessato.
La CRF sarà priva di dati identificativi del paziente ma recherà solo il codice identificativo.
La corrispondenza tra nominativo del paziente e il Codice univoco sarà registrata su file Excel separato

**Potenziali benefici derivanti dall'implementazione del sistema:**
Non sono previsti benefici diretti dalla sua partecipazione. Lo studio ha lo scopo di descrivere le caratteristiche dei pazienti, l'evoluzione delle malattie oggetto di osservazione ed eventuali effetti delle terapie.

**Potenziali rischi derivanti dall'implementazione del sistema:**
Per la natura osservazionale dello studio, non sono previsti rischi addizionali rispetto a quelli già noti in relazione al normale trattamento di questa tipologia di pazienti.
Vi è un potenziale rischio aggiuntivo di accesso illegittimo ai dati, che saranno protetti come sotto descritto in modo da minimizzare i rischi di trattamento.

### 3.1.2 Fasi del processo

#### *3.1.2.1 Progettazione (definizione del protocollo)*

Nella fase di progettazione è stata individuata una platea di soggetti rispondenti a determinati criteri (criteri di eligibilità) e di un numero di pazienti che possa dare significatività statistica allo studio. Il numero di pazienti è stato individuato, complessivamente nel protocollo, in un range di circa 75.
Sono stati individuati:

- Le ricerche già effettuate in materia
- Il set di dati da raccogliere
- Le correlazioni ipotizzate tra le diverse variabili

La fase di progettazione si è conclusa con la predisposizione del protocollo dello studio che ha tenuto conto dei seguenti elementi:

- I criteri di eleggibilità
- I numeri dei soggetti da coinvolgere
- La valutazione della possibilità di informare gli interessati ed acquisire il relativo consenso.
  Si rimanda all'Autorizzazione Generale sulla ricerca scientifica1 per un'esemplificazione dei suddetti casi:

[1] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9068972#5 Negli altri casi, quando non è possibile acquisire il consenso degli interessati, i titolari del trattamento devono documentare, nel progetto di ricerca, la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali 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, tra le quali in particolare:

1. i motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione dello studio la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento).

2. i motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui lo studio riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute).

Con riferimento a tali motivi di impossibilità organizzativa, le seguenti prescrizioni concernono anche il trattamento dei dati di coloro i quali, all'esito di ogni ragionevole sforzo compiuto per contattarli, anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente, risultino essere al momento dell'arruolamento nello studio: deceduti o non contattabili.

- Deceduti
- Non contattabili
- Non in grado di comprendere l'informativa stessa e/o esprimere un valido consenso

- I dati di partenza
- I dati da raccogliere per lo studio (dettaglio della CRF Case Report Form)
- La relativa codifica (IDC, etc.)
- La precisione dei dati da raccogliere
- Le procedure di data quality applicabili
- Il periodo di conservazione dei dati al termine dello studio (7 anni)
- L'elenco dei soggetti coinvolti
- L'individuazione degli strumenti di trattamento applicabili nelle diverse fasi
- Le procedure di eventuali scambi dati con altri soggetti
- Le norme che richiedono/su cui si basa la ricerca
- Gli standard applicabili
- I ruoli privacy
- Altri aspetti privacy (informativa, consenso, trasferimenti, rispetto dei principi)

La fase di progettazione ha tenuto conto dei requisiti degli artt. 5 e 25 del GDPR, per il cui dettaglio si rinvia al par. 4 - Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento.

#### *3.1.2.2 Fase di individuazione dei pazienti eleggibili*

Tale fase prevede, almeno come primo step, la consultazione delle seguenti basi dati: cartelle cliniche cartacee o online, referti di indagini biochimiche e microbiologiche tramite i corrispettivi applicativi aziendali dedicati.
La consultazione viene condotta dal personale, esperto e adeguatamente formato, che partecipa alla Sperimentazione, producendo un'estrazione che contenga solamente:
I dati previsti dalla CRF, possibilmente già con la precisione e la codifica definite nello studio.
L'insieme dei dati di controllo previsti dalle procedure di data quality.

#### *3.1.2.3 Pseudonimizzazione*

Per quanto riguarda le tecniche di pseudonimizzazione utilizzate si rinvia al paragrafo 6.2.

In ogni caso, si considerano rispettati i criteri fissati dall'Allegato A5[2].

[2] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637 Art. 4.
Identificabilità dell´interessato. Agli effetti dell´applicazione delle presenti regole:
a) un interessato si ritiene identificabile quando, con l´impiego di mezzi ragionevoli, è possibile stabilire un´associazione significativamente probabile
b) tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati che la identificano;
c) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:
• risorse economiche;
• risorse di tempo;
• archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
• archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;
• risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;
• conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;
Art. 5. Criteri per la valutazione del rischio di identificazione 1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto anche dei seguenti criteri:
a) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;
b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;
c) i risultati statistici relativi a sole variabili pubbliche non sono soggette alla regola della soglia;
d) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;
e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;
f) si presume adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentano la medesima modalità di una variabile

### 3.1.2.4 *Fase di estrazione e copiatura nella CRF*

I dati clinici saranno estratti manualmente, a cura di personale esperto e adeguatamente formato e inseriti nella CRF su database Microsoft Excel su server aziendale.
Il sistema sarà gestita dal P.I. e Co-P.I con accesso con credenziali e PW.
I dati clinici saranno estratti manualmente dalle cartelle cliniche informatizzate/cartacee e dagli applicativi aziendali.
Nella CRF i dati personali dell'interessato non sono riportati in chiaro, ma esclusivamente mediante ID univoco associato all'anagrafica che identificherà i dati dell'interessato all'interno dei registri di studio. L'associazione ID/anagrafica è gestita e archiviata su un file excel differente da quello utilizzato per la raccolta.
Il file excel (aggiornato costantemente nel tempo alle versioni più recenti del pacchetto Office 365 secondo le procedure aziendali) sarà conservato all'interno dei PC aziendale dedicati, protetti da password, siti presso gli ambulatori dei Centri, nei quali l'accesso è limitato al personale autorizzato.
In ogni caso non possono essere introdotte chiavi che, anche in combinazione tra loro, portino all'identificazione diretta del paziente, anche facendo uso di informazioni tenute logicamente ed organizzativamente separate.

I centri satelliti utilizzeranno un file excel per l'invio alla ASST Promotore dei dati completamente pseudonimizzati. Per garantire la sicurezza della trasmissione i file excel verranno inviati via PEC (che garantisce la cifratura del canale di trasmissione), e si proteggeranno con password comunicata attraverso un canale alternativo (ad es. per messaggio o via mail ordinaria).

### 3.1.2.5 *Fase di data quality*

Gli obiettivi di questa fase sono:

- L'accuratezza dei dati inseriti nella CRF
- La verifica che non vi è possibilità di single out di pazienti

Tale fase può comportare eventuali aggregazioni e/o nuove generalizzazioni (da notificare eventualmente al comitato etico) o l'esclusione dallo studio di pazienti eleggibili ma "singoli".
A valle di questa fase, i dati verranno anonimizzati/de-identificati per le finalità di pubblicazione scientifica.
Tuttavia, verrà comunque mantenuta l'associazione con i rispettivi dati anagrafici del paziente, al fine di poter risalire all'origine dei dati per effettuare studi di follow up per i pazienti oppure in caso di risultati scientifici che possano avere un impatto rilevabile per il soggetto stesso. L'esigenza potrebbe manifestarsi anche per provare alla comunità scientifica la validità della ricerca (peer review).

[2] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637 Art. 4.
Identificabilità dell´interessato. Agli effetti dell´applicazione delle presenti regole:
d) un interessato si ritiene identificabile quando, con l´impiego di mezzi ragionevoli, è possibile stabilire un´associazione significativamente probabile
e) tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati che la identificano;
f) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:
• risorse economiche;
• risorse di tempo;
• archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
• archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;
• risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;
• conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;
Art. 5. Criteri per la valutazione del rischio di identificazione 1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto anche dei seguenti criteri:
g) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero

un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;

h) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;
i) i risultati statistici relativi a sole variabili pubbliche non sono soggette alla regola della soglia;
j) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;
k) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;
l) si presume adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentano la medesima modalità di una variabile.

#### *3.1.2.6 Fase di correlazione statistica*

In questa fase si procede all'analisi statistica. Tipicamente sono utilizzate librerie di analisi statistica. Queste devono essere aggiornate e non comportare trasferimenti di dati a soggetti terzi.

Le analisi statistiche verranno eseguite utilizzando utilizzando il software Jamovi (the Jamovi project, versione 2,6 o successive, Sidney, Australia).La statistica delle variabili categoriche prevederà l'espressione di dati sotto forma di frequenze e l'utilizzo del test esatto di Fisher per i confronti tra gruppi.
Le variabili continue verranno espresse come mediana seguita da 10° e 90° percentile, assumendo per tali numerosità una distribuzione non normale ed il confronto tra gruppi verrà eseguito mediante test di Mann-Whitney o Wilcoxon per il confronto di dati appaiati.
Per il confronto tra gruppi per variabili continue e misure ripetute verrà utilizzato un robust linear mixed effect model.
Qualora la numerosità del gruppo di osservazione MPO-ILD lo consentirà (>15 pz), potrà essere effettuata un'analisi multivariata mediante modello di regressione logistica/Cox/lineare a seconda della natura dell'outcome.
Verrà eseguita un'analisi di sopravvivenza mediante curve di Kaplan-Meier e i gruppo verranno confrontati mediante il test di log-rank.
L'analisi statistica dei dati verrà eseguita direttamente dagli Sperimentatori.

#### *3.1.2.7 Fase di preparazione dei dati da pubblicare*

Obiettivo di questa fase è la verifica che i dati da pubblicare siano realmente anonimi, con probabilità di re-identificazione estremamente bassa, verificando che non vi è possibilità di single out di pazienti

#### *3.1.2.8 Fase di anonimizzazione/cancellazione dei dati*

Obiettivo di questa fase è assicurare la completa non collegabilità dei dati ai singoli pazienti.
In seguito, il P.I. presso il centro aderente ASST di Mantova procederà con la cancellazione sicura (fisica) di tutti i supporti (principali e copie di backup) su cui sono conservati i dati anagrafici dei pazienti.
Stante la natura e la finalità dello studio in oggetto, si ritiene opportuno conservare i dati per un periodo di 7 anni successivi al termine dello studio.

Presso il centro ASST di Mantova o presso il centro aderente si procederà con la cancellazione sicura (fisica) di tutti i supporti (principali e copie di backup del file excel) su cui sono conservati i dati anagrafici dei pazienti.

### 3.1.3 Ruoli e responsabilità collegate al trattamento

I soggetti che possono intervenire riguardo al trattamento sono, in qualità di titolari autonomi, tutti i centri partecipanti che ad oggi sono:

| Centro | Unità operativa |
|---|---|
| Azienda Socio Sanitaria Territoriale di Mantova – Promotore e coordinatore | Struttura Allergologia Immunologia Clinica e Reumatologia |
| Azienda Socio Sanitaria Territoriale del Garda | Struttura Pneumologia |
| Azienda Socio Sanitaria Territoriale di Crema | Struttura Pneumologia |
| Azienda Socio Sanitaria Territoriale Spedali Civili di Brescia | Struttura Pneumologia |

| | |
|---|---|
| Azienda Socio Sanitaria Territoriale Spedali Civili di Brescia | Struttura Reumatologia |
| Fondazione I.R.C.C.S. Policlinico San Matteo Pavia | Struttura Reumatologia |

Il Comitato Etico ed AIFA possono intervenire nel processo per le verifiche di competenza.

In ogni caso il personale che accede ad archivi contenenti dati personali, anche solo indirettamente identificativi, è stato autorizzato se subordinato/parasubordinato oppure nominato Responsabile ex art. 28 GDPR negli altri casi.

*3.1.3.1 Persone fisiche che intervengono nel trattamento presso il centro ASST Mantova*

Nel trattamento intervengono:

**L'investigatore/sperimentatore principale**: definisce il protocollo e assume il ruolo di designato/delegato, cioè di autorizzato con ruolo di impostazione e coordinamento.

**Co-sperimentatori:** coordinati dall'investigatore principale raccolgono i dati.

*3.1.3.2 Correlazione tra i soggetti e le fasi*

| Fase | Soggetti giuridici | Persone fisiche |
|---|---|---|
| 3.1.2.1 Progettazione (definizione del protocollo) | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |
| 3.1.2.2 Fase di individuazione dei pazienti eleggibili | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |
| 3.1.2.3 Pseudonimizzazione | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |
| 3.1.2.4 Fase di copiatura nella CRF | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |
| 3.1.2.5 Fase di data quality | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |
| 3.1.2.6 Fase di correlazione statistica | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |
| 3.1.2.7 Fase di preparazione dei dati da pubblicare | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |
| 3.1.2.8 Fase di anonimizzazione/ cancellazione dei dati | Ente Sperimentatore (Titolare) | Investigatore Principale/Co-Investigatori |

## 3.2 Dati, processi e beni di supporto

### 3.2.1 Dati trattati

Dati personali del paziente:

- Dati identificativi (ID paziente, età, sesso)
- Dati di contatto
- Dati relativi alla salute (Dati clinici anamnestici, Stadio della malattia alla Diagnosi, trattamenti e tipo di Immunoterapia, presenza o meno di tossicità, Informazioni terapeutiche)
- Risultati di analisi biochimiche e microbiologiche

- Dati di comorbidità e informazioni di follow-up (Esposizione a fumo o sostanze pneumotossiche, Comorbidità respiratorie e non, Vasculite ANCA associata e sintomi della stessa
- Prove di funzionalità respiratoria
- Anamnesi farmacologica: esposizione a terapia antifibrotica, immunosoppressiva o corticosteroidea
- Autoanticorpi
- Sopravvivenza

Relativamente ai pazienti, non verranno raccolti dati genetici.

Per l'adozione delle necessarie misure di sicurezza si trattano i seguenti dati degli operatori (es.: Investigators).

- Dati anagrafici (Nome e Cognome)
- Credenziali di accesso
- Fattore di autenticazione (password, token)
- Mail
- Log delle operazioni effettuate (data e ora di esecuzione, tipologia di operazione compiuta).

I log di windows registrano le operazioni di accesso al sistema da parte degli utenti.

| Dato | Interessato | Sistema di provenienza del dato | Forma |
|---|---|---|---|
| Log delle operazioni effettuate | | | Chiaro |

### 3.2.2 Fonti dei dati

I dati dei pazienti utilizzati per le finalità dello studio sono acquisiti da cartella clinica online o cartacea e applicativi informatizzati dedicati aziendali.

#### *3.2.2.1 Flusso dei dati*

I dati dei pazienti interni ed esterni alla ASST di Mantova rimarranno esclusivamente all'interno del presente Ente per tutta la durata dello studio.

*3.2.2.2*

Si veda il capitolo 3 - Fase 1: Descrizione del trattamento.

#### *3.2.2.3 Tipo di operazioni*

La tipologia delle operazioni effettuate sono:
**Operazioni standard:** Raccolta, Registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.
**Operazioni particolari**: nessuna
**Comunicazione mediante trasmissione:** I dati personali non sono comunicati a soggetti terzi.
**Profilazione:** Nell'ambito di tali trattamenti i dati personali non sono oggetto di processi decisionali automatizzati né di profilazione (ovvero una qualsiasi forma di trattamento automatizzato per valutare determinati aspetti personali, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica) su cui si basi una decisione o che produca un effetto giuridico sull'interessato o che incide significativamente sulla sua persona.

### 3.2.3 Beni di supporto

I beni di supporto possono essere raggruppati in:

- Fonti dei dati:

- database degli applicativi aziendali (Galileo; Dedalus, Firenze)

- Sistema per la gestione della CRF (CRF)
  - Fogli di calcolo Excel

- Infrastruttura:
  - Postazioni di lavoro (Computer dedicato – sistema operativo: Windows), fisicamente localizzato presso agli ambulatori di Pneumologia e Reumatologia della ASST Mantova.

# 4. Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento

## 4.1 Proporzionalità e necessità

Lo scopo di miglioramento del processo di cura/prevenzione e più in generale della salute della collettività si viene a contrappore al diritto alla riservatezza dei singoli. Il miglioramento è tanto più urgente quanto le patologie hanno effetti socioeconomici importanti. D'altra parte, gli impatti sui pazienti sono tanto maggiori quanto le patologie destano allarme sociale e potenziale discriminazione.
I dati personali sono indispensabili per la qualità della cura. Le fasi di verifica dei risultati sono un requisito fondamentale di un processo di qualità. Queste, quindi, richiedono una collegabilità del dato alle informazioni cliniche primarie e di conseguenza all'identità del paziente. La strategia principale per rendere il trattamento il meno impattante possibile sulla riservatezza è la minimizzazione della collegabilità tramite tecniche di minimizzazione e pseudonimizzazione dei dati.

### 4.1.1 Finalità esplicite e legittime

Le finalità del trattamento sono:

1. Di ricerca scientifica: valutazione di particolari protocolli sanitari, efficacia di protocolli di prevenzione, valutazione degli effetti di comorbilità.

### 4.1.2 Fondamenti legali del trattamento

La base giuridica del trattamento dei dati personali per le finalità di ricerca è così individuata:
- per i pazienti in vita e rintracciabili il consenso informato (art. 6, lett a) e art. 9, par. 2, lett. a) del GDPR)
e
- per i pazienti deceduti o non raggiungibili nell'art. 110, comma 1, ultimo capoverso del Codice privacy, articolo 9, paragrafo 2, lett. j) GDPR, artt. 36 e 89 GDPR.

Con riferimento ai pazienti deceduti o non contattabili il trattamento si rende necessario per le seguenti ragioni riconducibili a specifici motivi di impossibilità organizzativa:
a) Decesso dei pazienti: il numero stimato di interessati che non sarà possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella ricerca, è molto alto a causa dell'elevata incidenza della mortalità per la patologia oggetto dello studio.
b) Irreperibilità e/o limitata disponibilità degli indirizzi aggiornati dei pazienti: in aggiunta a quanto previsto nel precedente punto a), per i pazienti ancora in vita, non si può escludere l'eventualità che una parte risulti non contattabile anche all'esito di ogni ragionevole sforzo compiuto per rintracciarla. In tali casi si ritiene che lo sforzo necessario per raggiungere gli Interessati potrebbe richiedere un tempo eccessivo rispetto alla durata limitata dello studio la cui conclusione è prevista indicativamente dopo 12 mesi dall'avvio, pregiudicandone il conseguimento.
c) gli interessati risulteranno non contattabili solo all'esito di ogni ragionevole sforzo compiuto per rintracciarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente), che verrà documentato dal Medico Responsabile attraverso la compilazione di uno specifico modulo.

È altresì prevista la raccolta del consenso dell'Interessato non appena il paziente dovesse recarsi nuovamente presso il centro, anche per visite di controllo, anche al fine di consentire allo stesso di esercitare i diritti previsti dal Regolamento.
Al fine di garantire la tutela dei diritti, le libertà e i legittimi interessi degli Interessati non contattabili, si adotterà idonea forma di pubblicità dell'informativa ex art. 14 del Regolamento, secondo quanto previsto dall'art. 6 delle Regole Deontologiche (art. 6), mediante la pubblicazione dell'informativa medesima sul sito aziendale.
Inoltre, il Centro potrà dare inizio ai trattamenti dei dati personali necessari per la realizzazione dello studio solo dopo l'ottenimento del parere favorevole del Comitato etico territorialmente competente, in quanto elemento della condizione di liceità del trattamento dei dati personali per le finalità dello Studio, laddove non sia possibile acquisire il consenso degli interessati.

#### 4.1.3 I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario al conseguimento delle finalità del trattamento ("Minimizzazione dei dati")

Ogni dato raccolto è direttamente e specificatamente funzionale alle necessità per le quali è stato raccolto ed è pertanto pertinente rispetto alle finalità sopra esplicitate.

#### 4.1.4 Accuratezza ed aggiornamento dei dati

Gli Sperimentatori verificano la correttezza dei dati raccolti sulla scheda raccolta dati confrontandoli con quelli presenti sulla cartella clinica del partecipante. I dati sono raccolti e trattati da un numero ristretto di persone: dal Principal Investigator e Co-Investigator.
Si assume che la documentazione clinica di origine (cartella clinica) sia accurata (documento di fede privilegiata).
Le procedure di data quality previste sono tese a verificare queste proprietà del dato.

- Pseudonimizzazione: i dati verranno trattati mediante processo di pseudonimizzazione, ovvero ad ogni soggetto partecipante allo studio verrà assegnato un codice che verrà utilizzato nello studio, come descritto nel paragrafo 6.2. (i dati contenuti nella Base Dati sono infatti pseudonimizzati e non permettono quindi di risalire direttamente all'identità degli Interessati. I dati contenenti la corrispondenza tra i dati anagrafici dei pazienti e il codice identificativo sono infatti salvati separatamente).
  La chiave per risalire all'oggetto sarà conosciuta solo dai Principal Investigators e dai ricercatori del gruppo di ricerca autorizzati dal PI.

- Anonimizzazione: I dati raccolti saranno oggetto di un'attività di anonimizzazione, sulla base del WP 216 5/2014 per la pubblicazione e alla fine dello studio.

#### 4.1.5 Durata della conservazione dei dati

I dati in forma direttamente identificabile sono conservati a norma di legge nella documentazione clinica (ambito escluso dalla presente DPIA).
La tabella di conversione contenente i dati anagrafici e direttamente identificativi del paziente verrà distrutta subito dopo l'inserimento dei dati in CRF.
I dati conservati nella CRF saranno conservati in modalità segregata per 7 anni dopo il termine dello studio sotto forma di backup creato dal sistema. La CRF verrà chiusa al termine dello studio, in seguito non saranno più consentiti accesso e modifiche alla CRF.
Tale periodo di conservazione si rende necessario al fine di costruire analisi e studi futuri, volti a migliorare le conoscenze demografiche, cliniche, diagnostiche e terapeutiche e la pratica clinica.
I risultati dello studio (dati anonimi) verranno conservati a tempo indeterminato.
È fatta salva la conservazione dei dati personali, anche particolari, per un periodo superiore, nei limiti del termine di prescrizione dei diritti, in relazione ad esigenze connesse all'esercizio del diritto di difesa in caso di controversie.

## 4.2 Controlli per proteggere i diritti degli interessati

### 4.2.1 Come sono informati gli interessati circa il trattamento

Gli interessati saranno informati mediante l'informativa ex art. 13 GDPR verrà pubblicata sul sito web istituzionale della ASST Mantova, con richiamo nella sezione News e in un box dedicato, al fine di fornire adeguata pubblicità del trattamento per tutti i casi di impossibilità di contatto con i singoli interessati (o di altre ragioni per la non acquisizione del consenso), in ossequio alle regole deontologiche sulla ricerca scientifica Allegato A5 Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 - 19 dicembre 2018.
Si rinvia all'Allegato 1.0 per la consultazione delle informative.

### 4.2.2 Esercizio dei diritti da parte degli interessati

Per esercitare i diritti previsti dagli artt. da 15 a 22 del GDPR, l'interessato può rivolgersi al titolare del trattamento, anche per il tramite del DPO. I diritti possono essere esercitati con le modalità indicate nell'informativa.
Inoltre, come precisato nell'informativa, l'interessato può sempre esercitare, qualora ritenga che il trattamento dei Suoi dati personali avvenga in violazione di quanto previsto dal GDPR, il diritto di proporre reclamo all'Autorità di controllo, seguendo le indicazioni pubblicate sul sito della stessa (https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo) o di ricorrere avanti la competente autorità giudiziaria (artt. 77 e 79 del GDPR).

*4.2.2.1 Diritto di accesso*

Con riferimento al diritto di accesso, l'interessato può ottenere la conferma che sia o meno in corso un trattamento di dati che lo riguardano e in tal caso ottenere l'accesso agli stessi e alle informazioni riportate in dettaglio all'art. 15 del GDPR (es. finalità, destinatari, periodo di conservazione).

*4.2.2.2.Diritto di rettifica*
L'interessato, inoltre, ha sempre il diritto di ottenere – senza ingiustificato ritardo e comunque entro un mese - la rettifica dei dati personali inesatti che lo riguardano ovvero l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

*4.2.2.3.Diritto di cancellazione*
Per il trattamento in oggetto che si fonda sul consenso, l'interessato potrà richiedere la cancellazione dei dati personali nell'ambito del presente studio, ai sensi dell'art. 17 del GDPR.
Per quanto concerne, invece, il trattamento dei personali fondato sull'art. 110 del Codice Privacy, il diritto alla cancellazione dei dati potrà essere esercitato anche per il tramite dei soggetti legittimati ai sensi dell'art. 2-terdecies del Codice Privacy.

*4.2.2.4.Diritti di limitazione*
L'interessato ha il diritto di chiedere la limitazione del trattamento quando:

a. contesta l'esattezza dei dati personali, chiedendo quindi la rettifica, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
b. ritiene che il trattamento sia illecito e chiede che ne sia limitato l'utilizzo;
c. i dati personali sono necessari per l'accertamento, l'esercizio o la difesa di un diritto dell'interessato in sede giudiziaria;
d. si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

*4.2.2.5 Diritto di opposizione*
L'interessato ha il diritto di opporsi al trattamento per motivi connessi alla sua situazione particolare. Il

Titolare dovrà astenersi dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. (art. 21 del GDPR).

#### 4.2.3 Obbligazioni dei responsabili del trattamento

L'investigatore principale è stato individuato quale responsabile del trattamento *ex* art. 28 del GDPR.

### 4.3 Trasferimenti al di fuori dello SEE

Non vengono effettuati trasferimenti al di fuori dello Spazio Economico Europeo.

### 4.4 Rispetto dei principi di Privacy by Design

#### 4.4.1 Rispetto delle strategie

a. Minimizzare: sono trattati soltanto i dati necessari per raggiungere le finalità
b. Aggregare: sono applicate misure di pseudonimizzazione che prevedono tale strategia
c. Nascondere: il trattamento dei dati personali è limitato soltanto a soggetti autorizzati ed i dati vengono conservati in forma cifrata
d. Informare: all'interessato sono fornite tutte le informazioni pertinenti al trattamento in oggetto (informative ex artt. 13 e 14 GDPR)
e. Controllare: all'interessato è garantito l'esercizio dei diritti previsti dalla normativa (artt. 15- 22 GDPR). Si rinvia alla procedura di gestione dei diritti degli interessati.
f. Dimostrare: si rinvia alle policy del Titolare del trattamento

## 5. Fase 3: Calcolo del livello del rischio

Il livello del rischio viene calcolato moltiplicando il valore dell'Impatto (conseguenze negative per gli Interessati di una determinata minaccia) per la Probabilità che una determinata minaccia si possa verificare.
Pertanto, il livello del rischio è pari:

**LIVELLO DEL RISCHIO = IMPATTO X PROBABILITÀ OCCORRENZA DELLA MINACCIA**

### 5.1 Individuazione delle misure che mitigano il rischio

Determinato il livello del rischio, e individuate le minacce e le fonti che potrebbero concretizzarlo, vengono individuate ora le misure di sicurezza che contribuiscono alla mitigazione del rischio stesso.

**Perdita di riservatezza**

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

| |
|---|
| Le principali minacce relative alla perdita di riservatezza riguardano comportamenti umani quali, ad esempio, condivisione dei dati personali con soggetti non autorizzati, errori nelle configurazioni di sicurezza dei sistemi informatici che permettono accessi illegittimi, attacchi informatici esterni, violazione di account. |

**Quali sono le fonti di rischio?**

| |
|---|
| Le fonti di rischio sono quindi costituite principalmente da operatori interni mal istruiti o insoddisfatti, attacchi esterni tramite phishing, social engineering o sfruttamento di vulnerabilità. Oltre alla condivisione dei dati personali con soggetti non autorizzati, errori nelle configurazioni di sicurezza dei sistemi informatici che permettono accessi illegittimi, attacchi informatici esterni, violazione di account |

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

La probabilità di accadimento delle minacce è mitigata da diverse misure che verranno descritte nel dettaglio nel paragrafo 6. In particolare, le misure che maggiormente contribuisco a garantire una maggior tutela della riservatezza sono la pseudonimizzazione, la prevenzione del malware, la MFA e la segmentazione di rete.

a) I dati contenuti nella Base Dati sono infatti pseudonimizzati e non permettono quindi di risalire direttamente all'identità degli Interessati. I dati contenenti la corrispondenza tra i dati anagrafici dei pazienti e il codice identificativo sono infatti salvati separatamente, come indicato nella sezione dedicata al Partizionamento.
b) Inoltre, gli accessi ai dati personali da parte degli utenti finali della Piattaforma sono permessi solo a seguito di autenticazione tramite password e, in alcuni casi, tramite autenticazione a due fattori (TFA – Two Factor Authentication) attribuendo i permessi sulla base dei ruoli ricoperti.
c) Gli accessi fisici sono controllati e le postazioni gestite.
d) Viene erogata regolare formazione agli autorizzati al trattamento.

Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, gestione del personale, vulnerabilità.

**Perdita d'integrità**

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

Le principali minacce relative alla perdita di integrità riguardano ridotti controlli di qualità sulle procedure di data entry. L'errore più probabile potrebbe essere un errore nel mappaggio tra il dato originale e la codifica standard di riferimento. I rischi potrebbero, inoltre, concretizzarsi a seguito di attacchi informatici ed errori umani.

**Quali sono le fonti di rischio?**

Le fonti di rischio principali riguardano: un operatore interno mal istruito o insoddisfatto, attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità.

**Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?**

Le misure, meglio descritte nel paragrafo 6, adottate per mitigare i rischi di perdita d'integrità sono le seguenti

- Prima di tutto vengono eseguiti diversi controlli di qualità sui dai (descritti alla sezione 3.1.2.5) che ne garantiscono l'integrità: controlli di qualità a campione.
- Gli accessi ai dati personali sono permessi solo a seguito di autenticazione attribuendo i permessi sulla base dei ruoli ricoperti.
- Gli accessi fisici sono controllati e le postazioni gestite.

Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, crittografia, vulnerabilità.

**Perdita di disponibilità**

**Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?**

La principale minaccia relativa alla perdita di disponibilità riguarda la distruzione accidentale della Base Dati o fisica del server.

**Quali sono le fonti di rischio?**

Le fonti di rischio per una perdita di disponibilità sono: attività volontaria di un operatore interno con accesso alla Base Dati; attaccante esterno tramite phishing, social Engineering o sfruttamento di vulnerabilità. Errore umano interno per disattenzione/incompetenza. Perdita della password.

**Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?**

Le misure adottate per mitigare la perdita di disponibilità dei dati, meglio descritte nel paragrafo 6, riguardano principalmente la presenza di backup giornalieri dei dati e test periodici del sistema di ripristino. Sono, inoltre, implementate le seguenti misure che contribuiscono alla mitigazione del rischio: controlli degli accessi logici e degli accessi fisici, archiviazione, partizionamento, tracciabilità, minimizzazione dei dati, sicurezza dei canali informatici, gestione degli incidenti di sicurezza e delle violazioni dei dati personali, sicurezza dell'hardware, vulnerabilità, lotta contro il malware, gestione postazioni, gestione dei rischi, gestione del personale, sicurezza dei canali informatici, sicurezza dell'hardware e vigilanza sulla protezione dei dati.

# 6. Fase 4: Misure di mitigazione adottate

Vengono implementate le seguenti tecniche di cifratura dei dati personali:

## 6.1 Crittografia - Cifratura

Viene istituita una password individuale per il personale autorizzato per l'accesso al database Microsoft Excel. Il file relativo alle corrispondenze e il database in excel saranno protetti tramite password differenti.

I criteri di robustezza sono:
 Lunghezza minima 14 caratteri
 Lettere maiuscole e minuscole
 Cifre di base 10 (da 0 a 9)
 Caratteri non alfanumerici
Vengono implementate tecniche di pseudonimizzazione.

## 6.2 Pseudonimizzazione

Al fine di ottenere la separazione tra i dati identificativi del paziente e i dati della eCRF implementata nel database (ciascun paziente incluso nella eCRF viene assegnato un identificativo paziente progressivo univoco (Codice ID numerico) contestualmente all'ingresso del paziente nello studio.
Lo Sperimentatore Principale e lo Study Coordinator avranno accesso alla corrispondenza tra tale ID e l'identificativo univoco ospedaliero del paziente, che verrà conservato in un file separato (Subject Enrolment Log) conservato in uno storage protetto e gestito da personale autorizzato dal Titolare.

Nello specifico, i dati relativi al paziente saranno:
1. Informazioni relative al record paziente;
2. Informazioni relative al record diagnosi e situazione clinica del paziente secondo score prognostico di riferimento
3. Dati biochimici e microbiologici come da protocollo di studio

Il responsabile dei dati e della loro pseudonimizzazione sono lo sperimentatore principale e i co-sperimentatori.

## 6.3 Controllo degli accessi logici

Per gli accessi degli "amministratori di sistema" vengono applicate le disposizioni di cui al provvedimento del garante del 2008 e della circolare AGID per le misure di sicurezza della 18/04/2017.

Infrastruttura aziendale:
La sicurezza degli accessi prevede l'identificazione degli utenti tramite le credenziali nominative di dominio e la concessione del pertinente profilo di autorizzazione, determinato sulla base dei privilegi concessi al singolo utente.
Per gli accessi degli "amministratori di sistema" vengono applicate le disposizioni di cui al provvedimento del garante del 2008 e della circolare AGID per le misure di sicurezza della 18/04/2017.
In particolare, vengono implementate le seguenti tecniche di autenticazione dei dati personali:

- L'accesso ai dati della CRF è protetto tramite utilizzo di una password per il database Access/Excel.
- Il file relativo alle corrispondenze e il database Access/Excel saranno protetti tramite password differenti con criteri di robustezza quali:
    - Lunghezza minima 14 caratteri
    - Lettere maiuscole e minuscole
    - Cifre di base 10 (da 0 a 9)

Caratteri non alfanumerici

## 6.4 Tracciabilità

Le informazioni riguardanti i pazienti in studio verranno conservate per 7 anni sui server del Titolare.
Vengono tracciati e conservati per un anno i log di eventi di possibile rischio di sicurezza.

## 6.5 Minimizzazione dei dati

La raccolta dei dati si limita a quelli strettamente necessari a perseguire le finalità del trattamento.
Le fasi di progettazione dello studio ha implicato il rispetto del principio di minimizzazione.
Lo sperimentatore garantisce che i dati previsti nella CRF sono i soli indispensabili alla conduzione dello studio
L'esperto statistico garantisce che il numero di interessati è il minimo per dare rilievo allo studio.

## 6.6 Lotta contro il malware

Il computer sarà su dominio locale e disporrà delle ultime patch di sicurezza nonché antivirus aziendale aggiornato secondo le policy aziendali.
È pianificato specifico audit sulla configurazione dell'apparato.
Ciascuna postazione di lavoro è dotata di software antivirus, costantemente aggiornato in modo automatico.
Sono state impartite specifiche disposizioni per verificare puntualmente l'aggiornamento sui sistemi interessati.

## 6.7 Vulnerabilità

Inoltre, la protezione contro le vulnerabilità è garantita attraverso le seguenti attività:

- formazione del personale incaricato al trattamento dei dati
- aggiornamento del sistema con cadenza dettata dalla disponibilità di bollettini di sicurezza
- utilizzo di software e sistemi operativi supportati dal produttore
- piani di risposta agli incidenti
- piattaforma di gestione centralizzata delle vulnerabilità e monitoraggio.

## 6.8 Backup

Il Titolare è responsabile delle procedure di backup a livello di virtualizzazione o, copia periodica del server applicativo e del database, dove sono impostati backup giornalieri, mensili e annuali e retention di almeno 7 gg su server separati.

## 6.9 Archiviazione

I dati trattati tramite fogli di calcolo Excel sono conservati su server aziendale accessibile dalle postazioni PC poste negli ambulatori chiusi a chiave, accessibili solo dal personale autorizzato.
Le password per l'accesso ai file excel verranno custodite presso i locali in apposito luogo sicuro sotto la responsabilità del Principal investigator e Co-PI.
I dati vengono conservati sui server del Titolare fino a 7 anni successivi alla loro raccolta nella eCRF.

## 6.10 Sicurezza dei documenti cartacei

I dati cartacei sono conservati presso Ambulatorio della Struttura Allergologia. L'ufficio dispone di armadio con chiusura a chiave, accessibile solo dal personale autorizzato.

## 6.11 Sicurezza dell'hardware

Il computer, su dominio locale dispone delle ultime patch di sicurezza. Sono applicate le opportune configurazioni di sicurezza relative all'hardware.

## 6.12 Gestione postazioni

La gestione delle postazioni comprende la postazione di lavoro dedicata, fisicamente localizzata presso lo studio del Principal Investigator che viene chiuso a chiave.
Al computer dedicato per le attività avranno accesso solo il Principal Ingestigator e i Co-Sperimentatori.
Il computer resterà acceso solo durante il suo utilizzo.

Il Titolare ha predisposto un Regolamento per l'utilizzo dei dispositivi informatici, il quale prevede l'applicazione di:
-misure organizzative: istruzioni impartite agli operatori (blocco della postazione, spegnimento ordinato

all'uscita, divieto d'installazione di software non autorizzato, etc.)
-misure tecniche: antivirus, aggiornamenti di sistema operativo, etc.

### 6.13 Manutenzione

Il Titolare del trattamento è responsabile del piano di manutenzione ordinaria ed eventualmente evolutiva dei dispositivi hardware.

### 6.14 Controllo degli accessi fisici

Gli studi/ambulatori dove è ubicata la postazione fissa sono accessibili solo a personale autorizzato.

### 6.15 Protezione contro fonti di rischio non umane

La presenza di backup giornalieri, mensili ed annuali e retention di almeno 7 gg su server separati evita la perdita di dati.
Eventuali altri controlli legati a guasti, difetti dell'architettura IT, alimentazione, rischi ambientali sono demandati al responsabile dello studio

### 6.16 Misure di sicurezza in caso di trasferimenti verso Paesi non adeguati

Non sono previsti trasferimenti al di fuori dello Spazio Economico Europeo.

### 6.17 Politica di tutela della privacy

Le politiche privacy del Titolare del trattamento e dei responsabili del trattamento, relative alla propria organizzazione, sono conformi al GDPR.

### 6.18 Gestione dei rischi

È stata effettuata la valutazione dei rischi i cui risultati sono nello specifico paragrafo.

### 6.19 Integrare la protezione della privacy nei progetti

La fase di progettazione ha tenuto conto dei requisiti di privacy by design.
Per i pazienti contattabili, considerato che il trattamento riguarda dati sulla salute per scopi di ricerca medica, la base giuridica del trattamento si rinviene nel consenso, ai sensi dell'art. 9, par. 2, lett. a) del Regolamento.
Il Titolare ha verificato che non è possibile informare tutti gli interessati ed acquisirne il consenso, pertanto procede al trattamento dei dati personali in conformità con l'articolo 110 del Codice della privacy, quale condizione di liceità del trattamento per la parte di soggetti arruolabili la cui raccolta del consenso risulti impossibile.
Il Titolare ha svolto una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) dando evidenza dell'impossibilità o delle difficoltà oggettive in merito alla raccolta del consenso per i pazienti deceduti/non rintracciabili, come prescritto dall'articolo 35 del GDPR e in conformità con le nuove disposizioni dell'articolo 110 del Codice della privacy, assicurando che tutte le misure necessarie per mitigare i rischi associati al trattamento dei dati personali siano state identificate e implementate.
Il Titolare la fa propria avendo verificato l'implementazione delle misure di mitigazione previste.
Oltre all'approvazione da parte del Comitato Etico, il Titolare procederà con la pubblicazione della DPIA e specifica comunicazione all'Autorità Garante.

### 6.20 Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Titolare ha adottato le seguenti procedure aziendali in materia di trattamento dei dati personali:

- Gestione delle violazioni di dati personali
- Gestione dell'esercizio dei diritti dell'interessato

### 6.21 Gestione del personale

Il Titolare ha provveduto ad autorizzare il personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati).

Inoltre, ha provveduto a comunicare la disponibilità di procedure privacy al personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Le Procedure sono reperibili sulla intranet aziendale.
Sono state svolte attività di formazione (formazione obbligatoria) per tutto il personale che a vario titolo è coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Inoltre, pianifica annualmente gli interventi formativi.

### 6.22 Gestione dei terzi che accedono ai dati

Il CET potrà eventualmente accedere ai dati nello svolgimento dei suoi compiti istituzionali. I dati potranno essere richiesti in via teorica sulla base del L.241/90 da specifici portatori di interesse e con le relative cautele normativamente previste.

### 6.23 Vigilanza sulla protezione dei dati

Il Titolare ha nominato un DPO con il compito di vigilare sui trattamenti dei dati personali.

## 7. Fase 5: Consultazione dei rappresentanti e degli interessati

Nello svolgimento della DPIA, il Titolare, valutate le specifiche circostanze del trattamento in esame, ha ritenuto non necessario e sconveniente provvedere alla raccolta delle opinioni dei rappresentanti dei soggetti interessati in quanto:
- in parte si tratta di soggetti difficilmente contattabili o deceduti;
- in parte è possibile illustrare gli scopi e modalità dello studio durante la raccolta del consenso degli arruolati contattabili.

## 8. FASE 6. Calcolo del rischio residuo, piano di remediation e parere del DPO

### 8.1 Rischio residuo

Si ritiene che il rischio residuo collegato al trattamento di dati personali per le finalità dello studio in oggetto sia accettabile in quanto sono state adottate misure di sicurezza tecniche e organizzative idonee a contenere il rischio per i diritti e le libertà degli interessati.

### 8.2 Piano di remediation

Per la minimizzazione del rischio residuo, non sono al momento previste ulteriori misure di sicurezza.

### 8.3 Opinione del DPO

Il DPO ha espresso un parere in merito al presente documento che è conservato agli atti dell'Ufficio Affari Generali/Privacy.

## 9. FASE 7. Consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR

Dato che il trattamento dei dati personali rientra nei casi previsti dall'art. 110 del D.lgs 196/2003, il Titolare procederà alla consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR.

## 10. FASE 8. Monitoraggio e riesame nel tempo della DPIA

Ai sensi del paragrafo 11 dell'art. 35 del GDPR, il Titolare deve:
- verificare che il trattamento dei dati personali sia effettuato conformemente alla DPIA. A tal fine il DPO effettuerà degli audit con cadenza annuale;
- procedere a un riesame del trattamento oggetto di DPIA quando vengono apportate modifiche al trattamento con conseguente variazione del livello di rischio connesso al trattamento stesso, al fine

di valutare la necessità di apportare revisioni al DPIA Report ovvero di effettuare una nuova DPIA.

Per valutare se il livello di rischio è variato, si dovrà verificare se sono stati modificati uno o più dei seguenti aspetti:

- Cambiamento sulle attività di trattamento, in termini di:
  - contesto (variazione della localizzazione fisica o di elementi ambientali dell'azienda, nuovi vincoli, funzioni e struttura organizzativa, innesto di politiche e processi aziendali, leggi, norme e contratti);
  - modalità di raccolta dei dati personali (mediante modulo cartaceo o form elettronico, direttamente dall'interessato o indirettamente da terzi)
  - finalità del trattamento;
  - tipologia di dati personali trattati (ad esempio dati genetici);
  - categorie di interessati;
  - soggetti coinvolti nel trattamento (personale interno all'organizzazione o fornitori esterni);
  - combinazioni di dati (integrazione con dati provenienti da altre sorgenti, correlazione di informazioni censite su diverse basi dati);
  - trasferimento di dati all'estero (all'interno della UE o verso paesi od organizzazioni internazionali al di fuori della UE).
  - Modifica ai rischi con impatti sui diritti e le libertà delle persone fisiche, derivanti da:
  - Modifica dei sistemi informativi a supporto (subentro di un nuovo Service Provider, migrazione di servizi in Cloud, ecc.);
  - nuovi scenari di rischio (furti di identità e frodi informatiche, introduzioni di attacchi avanzati e azioni non autorizzate)
  - insorgenza di potenziali impatti sulle qualità di riservatezza, integrità e disponibilità dei dati personali;
  - nuove minacce (naturali, ambientali, tecniche, di terrorismo o sabotaggio, provenienti da comportamenti volontari o accidentali);
  - attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali;
  - dismissione di elementi di presidio esistenti.

- Mutamenti nel contesto organizzativo o sociale per l'attività di trattamento, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione.

A seguito delle predette verifiche dovrà essere calcolato il livello di rischio (utilizzando la procedura di cui al punto 4) e acquisito il parere del DPO in merito alla necessità di aggiornare la DPIA ovvero procedere ad una nuova valutazione d'impatto.

In ogni caso, anche a prescindere da modifiche apportate al trattamento, quest'ultimo sarà oggetto di riesame annuale, al fine di verificate se, a seguito di cambiamenti nelle conoscenze tecnico- scientifiche, si sia modificato il livello di rischio e sia quindi necessario adottare misure tecnico organizzative nonché rivedere/integrare la DPIA al fine di mantenere la validità e l'aggiornamento nel tempo della valutazione condotta e dei suoi risultati.

Allegati:

- Protocollo studio_V1 14.05.2026

- Foglio informativo e consenso_V1.0 14.05.2026

-Informativa e consenso trattamento dati_V1.0 14.05.2026