Versione 1.0 data 19.02.2026

Valutazione di IMPATTO

studio dal titolo "Valutazione della persistenza in trattamento della classe di farmaci IL-23 per la psoriasi nella pratica clinica corrente" PsO IL23

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	19.02.2026	---	Nessuna	Prima versione

Sommario

1. Informazioni generali ... 3
1.1 Titolare del trattamento ... 3
1.2 Contesto di riferimento ... 3
1.3 Standard di riferimento per la predisposizione della DPIA ... 3
1.4 Descrizione del quadro normativo e regolatorio, standard e buone prassi ... 4
1.5 Procedura per la conduzione della DPIA ... 5
2. Fase 0: Determinazione della necessità di condurre la DPIA e costituzione del team DPIA ... 5
2.1 Necessità di svolgere la DPIA ... 5
2.2 Piano delle attività ... 5
3. Fase 1: Descrizione del trattamento ... 6
3.1.1 Il trattamento oggetto della Valutazione di Impatto ... 6
3.1.2 Fasi del processo ... 6
3.1.3 Ruoli e responsabilità collegate al trattamento. ... 9
3.2 Dati, processi e beni di supporto ... 10
3.2.1 Dati trattati ... 10
3.2.2 Fonti dei dati ... 11
3.2.3 Beni di supporto ... 11
4. Fase 2: Valutazione necessità, proporzionalità e legittimità del trattamento ... 12
4.1 Proporzionalità e necessità ... 12
4.1.1 Finalità esplicite e legittime ... 12

4.1.2 Fondamenti legali del trattamento 12
4.1.3 I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario al conseguimento delle finalità del trattamento (“Minimizzazione dei dati”) 12
4.1.4 Accuratezza ed aggiornamento dei dati 12
4.1.5 Durata della conservazione dei dati 13
4.2 Controlli per proteggere i diritti degli interessati 13
4.2.1 Come sono informati gli interessati circa il trattamento 13
4.2.2 Esercizio dei diritti da parte degli interessati 13
4.2.3 Obbligazioni dei responsabili del trattamento 14
4.3 Trasferimenti al di fuori dello SEE 14
4.4 Rispetto dei principi di Privacy by Design 14
4.4.1 Rispetto delle strategie 14
5. Fase 3: Calcolo del livello del rischio 14
5.1 Individuazione delle misure che mitigano il rischio 14
6. Fase 4: Misure di mitigazione adottate 17
6.1 Crittografia - Cifratura 17
6.2 Pseudonimizzazione 17
6.3 Controllo degli accessi logici 17
6.4 Tracciabilità 17
6.5 Minimizzazione dei dati 17
6.6 Lotta contro il malware 17
6.7 Vulnerabilità 18
6.8 Backup 18
6.9 Archiviazione 18
6.10 Sicurezza dei documenti cartacei 18
6.11 Sicurezza dell'hardware 18
6.12 Gestione postazioni 18
6.13 Manutenzione 18
6.14 Contratto con il responsabile del trattamento 19
6.15 Controllo degli accessi fisici 19
6.16 Protezione contro fonti di rischio non umane 19
6.17 Misure di sicurezza in caso di trasferimenti verso Paesi non adeguati 19
6.18 Politica di tutela della privacy 19
6.19 Gestione dei rischi 19
6.20 Integrare la protezione della privacy nei progetti 19
6.21 Gestire gli incidenti di sicurezza e le violazioni dei dati personali 19
6.22 Gestione del personale 19
6.23 Gestione dei terzi che accedono ai dati 20

6.24 Vigilanza sulla protezione dei dati 20
7. Fase 5: Consultazione dei rappresentanti e degli interessati 20
8. Fase 6: Calcolo del rischio residuo, piano di remediation e parere del DPO 20
8.1 Rischio residuo 20
8.2 Piano di remediation 20
8.3 Opinione del DPO 20
9. Fase 7: Eventuale consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR 42
20
10. Fase 8: Monitoraggio e riesame nel tempo della DPIA 21

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 partecipante dello studio promosso da IRCCS Policlinico San Donato – San Donato Milanese (MI) che ne ha determinato il protocollo, in virtù del quale ogni centro è Titolare autonomo relativamente ai dati di sua competenza.
Il Principal Investigator (Responsabile dello studio) presso il Promotore è il Dott. Giuseppe Caravella, Direttore Farmacia.
Il Principal Investigator (Responsabile dello studio) presso la ASST di Mantova è la Dott.ssa Roberta Chittolina, Dirigente Farmacista presso la Struttura Farmacia Ospedaliera e Territoriale Mantova.

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti presenti nel data base FILE F di ASST Mantova, per le finalità di conduzione dello studio multicentrico, retrospettivo, osservazionale, dal titolo "Valutazione della persistenza in trattamento della classe di farmaci IL-23 per la psoriasi nella pratica clinica corrente".

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;
- 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;
- 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];
- Provvedimento del 14 gennaio 2021 - Regione Veneto. Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica;
- Convenzione di Oviedo – "Convenzione per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazioni della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina", del 4 aprile 1997;
- 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";
- GPDP – "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", pubblicate sulla G.U. n. 11 del 14 gennaio 2019;
- 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: Eventuale 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.

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.

Team di lavoro
Il presente documento è stato redatto da un team composto da:

- Affari Generali e Controlli Interni - Ufficio privacy
- DPO (per le impostazioni metodologiche e per il parere sulla DPIA stessa).

Il protocollo dello studio è stato sottoposto al competente Comitato Etico Indipendente (CET Lombardia 1) IRCCS Policlinico San Donato – San Donato Milanese (MI) che ha rilasciato il parere favorevole per tutti i centri, compreso ASST Mantova, espresso nella riunione del 18/06/2025.

2.2 Piano delle attività

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

3. Fase 1: Descrizione del trattamento

3.1.1 Il trattamento oggetto della Valutazione di Impatto

Si tratta di uno studio osservazionale retrospettivo su farmaco, multicentrico.

Obiettivi dello studio sono descrivere i pazienti con psoriasi a placche (PsO) in trattamento con anti-interleuchina 23 (anti-L-23) e analizzare la persistenza in trattamento (drug survival), quale indicatore utilizzato nell'ambito della ricerca Real World che fornisce informazioni sull'efficacia del farmaco, la sua sicurezza e la soddisfazione del paziente.

Lo studio è basato sui dati delle dispensazioni dei farmaci inibitori di IL-23 nel paziente con psoriasi a placche già raccolti in modo routinario dalle farmacie ospedaliere (File F – Regione Lombardia).
La durata dello studio è pari a 12 mesi:
La Unità Operativa coinvolta è la Farmacia Ospedaliera e Territoriale.

La raccolta dati verrà eseguita tramite la piattaforma Redcap del Policlinico San Donato attraverso una e-CRF multicentrica, trasversale e pseudonimizzata (eCRF: https://projectredcap.org/software/).

Potenziali benefici derivanti dalla sperimentazione allo studio:

Descrivere i pazienti con psoriasi a placche (PsO) in trattamento con anti-interleuchina 23 (anti-L-23) e analizzare la persistenza in trattamento (drug survival), al fine di acquisire maggiori informazioni sull'efficacia del farmaco, la sua sicurezza e la soddisfazione del paziente.

Potenziali rischi derivanti dalla sperimentazione allo studio:

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 rischio aggiuntivo di accesso illegittimo ai dati di ricerca, 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 400, che abbiano ricevuto la prima prescrizione di anti IL-23 nel periodo gennaio 2023 – dicembre 2024. Per caratterizzare il paziente in base ai trattamenti biologici per la psoriasi prescritti precedentemente all'anti IL-23 si raccoglieranno i dati delle dispensazioni nel periodo di 5 anni precedenti (periodo di caratterizzazione).

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 di soggetti da coinvolgere: oltre il numero per la significatività statistica si è ipotizzato di aggiungere un margine per la gestione di eventi quali revoca del consenso, opposizione
- La valutazione della possibilità di informare gli interessati ed acquisire il relativo consenso. Si rimanda all'Autorizzazione Generale sulla ricerca scientifica[1] 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:

- 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 (7 anni) al termine dello studio Il backup del CRF tramite applicativo Redcap è settato a 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 della base dati File F – Regione Lombardia per l'estrazione dei dati relativi alle dispensazioni dei farmaci inibitori di IL-23 nel paziente con psoriasi a placche.
I pazienti sono individuati con i seguenti criteri di inclusione:
-Pazienti adulti con psoriasi a placche (PsO)
-Pazienti eleggibili al trattamento con anti-IL-23

La consultazione viene condotta dallo Sperimentatore principale 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.

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.

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

3.1.2.4 Fase di estrazione e copiatura nella CRF

I dati clinici saranno estratti manualmente, a cura dello Sperimentatore principale, adeguatamente formato, e inseriti in una e-CRF elettronica, multicentrica, trasversale e pseudonimizzata, gestita su piattaforma RedCap del Policlinico San Donato (eCRF: https://projectredcap.org/software/).
I dati sulla salute inseriti nella e-CRF saranno pseudonimizzati e gestiti mediante un ID univoco associato all'anagrafica che identificherà i dati dell'interessato all'interno dei registri di studio. L'associazione ID/anagrafica sarà gestita e archiviata su un file excel differente da quello utilizzato per la raccolta. Il file excel sarà conservato all'interno di PC aziendale dedicato, protetto da password, sito presso la U.O. Farmacia, al quale l'accesso è limitato al solo Sperimentatore principale.
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. Nello specifico, la CRF dovrà avere come chiave quella individuata nello step di pseudonimizzazione.

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 (K anonimato, L Diversity)

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" (per esempio un paziente molto anziano).

A valle di questa fase, i dati verranno anonimizzati/de-identificati per le finalità di pubblicazione scientifica.

---

[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.

3.1.2.6 Fase di correlazione statistica

In questa fase si procede all'analisi statistica e si confermano (o meno) le ipotesi dello studio. Tipicamente sono utilizzate librerie di analisi descrittiva. Queste devono essere aggiornate e non comportare trasferimenti di dati a soggetti terzi. L'analisi statistica è in capo al Datamanager/Statistico del Promotore.

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 (K anonimato, L Diversity).

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.
I dati personali saranno conservati per il periodo di tempo prescritto dalle vigenti normative in materia di conservazione dei dati personali e comunque non oltre il tempo necessario ad adempiere alle finalità della ricerca.
Stante la natura e la finalità dello studio in oggetto, si ritiene opportuno conservare la tabella di correlazione per un periodo di 7 anni successivi al termine dello studio, in conformità ai tempi stabiliti nel Massimario di conservazione e scarto adottato dal Titolare.
Allo scadere del termine i dati verranno distrutti o resi anonimi provvedendo alla cancellazione definitiva e irreversibile della corrispondenza tra il codice utilizzato sul dato e l'associazione di tale codice all'identità del partecipante. Si procederà quindi 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.

Il soggetto che può intervenire, oltre al Titolare del trattamento (ASST Mantova), è:

- Fornitore piattaforma Redcap: Responsabile del trattamento ex art. 28 GDPR per la gestione della eCRF

In qualità di titolari autonomi, oltre all'IRCCS Policlinico San Donato – San Donato Milanese (MI) – Promotore, l'altro centro coinvolto è ASST Papa Giovanni XXIII – Bergamo (BG).
Vi sono altri soggetti (Comitato Etico, AIFA) che 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.

3.1.3.1.1 Persone fisiche che intervengono nel trattamento presso il centro aderente ASST Mantova

Nel trattamento intervengono:

-L'investigatore/sperimentatore principale: applica il protocollo: assume il ruolo di designato/delegato.

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 principale (Titolare)	Investigatore Principale Promotore
3.1.2.2 Fase di individuazione dei pazienti eleggibili	Ente che ha Raccolto i dati (Titolare)	Investigatore Principale **A**SST Mantova
3.1.2.3 Pseudonimizzazione	Ente che ha raccolto i dati (Titolare)	Investigatore Principale **A**SST Mantova
3.1.2.4 Fase di copiatura nella CRF	Ente che ha Raccolto i dati (Titolare)	Investigatore Principale **A**SST Mantova
3.1.2.5 Fase di data quality	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale **A**SST Mantova
3.1.2.6 Fase di correlazione statistica	Ente che ha raccolto/ricevuto i dati (Titolare)	Statistico Promotore
3.1.2.7 Fase di preparazione dei dati da pubblicare	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale Promotore
3.1.2.8 Fase di anonimizzazione/ cancellazione dei dati	Ente che ha raccolto/ricevuto i dati (Titolare)	Investigatore Principale **A**SST Mantova

3.2 Dati, processi e beni di supporto

3.2.1 Dati trattati

I dati personali relativi ai pazienti arruolati sono definiti nel progetto "IPP" creato tramite applicativo REDCap.

Dati personali del paziente:

- Dati anagrafici: Nome, Cognome, data di nascita e data dell'esame (saranno raccolti all'interno di un file di conversione che verrà distrutto al termine della compilazione del CRF Redcap, come già specificato sopra)
- Dati relativi alla salute fisica o psichica.

Non verranno raccolti dati genetici.

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

- 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 REDCap registrano tutte le operazioni effettuate sulla eCRF e sui dati da parte degli utenti.

3.2.2 Fonti dei dati

I dati dei pazienti utilizzati per le finalità dello studio sono acquisiti da applicativo informatizzato dedicato aziendale – File F – Regione Lombardia.

3.2.2.1 Flusso dei dati

I dati saranno inviati dai centri partecipanti al Promotore tramite il caricamento su REDCap.

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.
Diffusione: I dati potranno essere diffusi in forma aggregata per pubblicazioni scientifiche.
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:
  - Applicativo informatizzato aziendale dedicato alla dispensazione farmaci File F – Regione Lombardia

- Sistema per la gestione della CRF:
  - (e-CRF): Applicativo RedCap (https://projectredcap.org/software).

- Infrastruttura:
  - Postazioni di lavoro (Computer dedicato – sistema operativo: Windows), fisicamente localizzato presso Farmacia, studio Sperimentatore principale;
  - Share di rete su server aziendale;
  - Firewall.

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 ricerca. 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: 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 si fonda su:

La base giuridica del trattamento dei dati personali del centro aderente ASST Mantova è l'art. 110-bis c.4 Codice privacy (D.lgs. 30 giugno 2003, n. 196), in virtù della recente nota interpretativa rilasciata dall'Autorità Garante per la protezione dei dati personali nelle FAQ dedicate alla ricerca scientifica del 6 giugno 2024, che estende una base giuridica tipica di un IRCSS anche a una ASST poiché il promotore è un IRCSS.

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 nel data base informatizzato - sistema File F Regione Lombardia. I dati sono raccolti e trattati da un numero ristretto di persone: solo Principal Investigator.
Si assume che la documentazione clinica di origine (data base informatizzato) 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 dal Principal Investigator.
- Anonimizzazione: I dati raccolti saranno oggetto di un'attività di anonimizzazione, 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).
I dati 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 stessa con le credenziali fornite al ricercatore per Redcap.
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, come detto in precedenza, 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 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 per la consultazione della informativa.

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

Redcap: Fornitore quale responsabile del trattamento *ex* art. 28 del GDPR con apposito atto di nomina.

4.3 Trasferimenti al di fuori dello SEE

I dati personali sono raccolti all'interno della e-CRF in forma pseudonimizzata e, quindi, è potenzialmente possibile ricondurre le informazioni all'identità dell'interessato. Il Responsabile del trattamento REDCap (individuato formalmente dal Promotore) ha la sede dello stabilimento principale in USA e il trasferimento avviene sulla base del DPF (Data Privacy Framework) a cui REDCap stessa ha aderito, nonostante la remota possibilità di re-identificazione degli interessati

4.4 Rispetto dei principi di Privacy by Design

4.4.1 Rispetto delle strategie

1. Minimizzare: sono trattati soltanto i dati necessari per raggiungere le finalità
2. Aggregare: sono applicate misure di pseudonimizzazione che prevedono tale strategia
3. Nascondere: il trattamento dei dati personali è limitato soltanto a soggetti autorizzati ed i dati vengono conservati in forma cifrata
4. Informare: all'interessato sono fornite tutte le informazioni pertinenti al trattamento in oggetto (informative ex artt. 13 e 14 GDPR)
5. 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.
6. 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.

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 tramite il modulo 'Data Quality Rules' previsto nella piattaforma REDCap.
- 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

6.1 Crittografia - Cifratura

Vengono implementate le seguenti tecniche di cifratura dei dati personali:

In transito:

- il protocollo di trasporto dei dati tra application server e dispositivo dell'utente è crittografato HTTPS e cifrato nelle connessioni VPN.

At rest:

- I dati nella eCRF sono protetti tramite l'utilizzo di una tecnica di autenticazione tramite password e autenticazione a due fattori (password + codice di verifica)) per il database in REDCap.

6.2 Pseudonimizzazione

Vengono implementate tecniche di pseudonimizzazione, al fine di limitare l'Identificabilità dei dati e ottenere la separazione tra i dati identificativi del paziente e i dati della eCRF implementata in REDCap.
A ciascun paziente incluso nella eCRF viene assegnato un ID numerico, contestualmente all'ingresso del paziente nello studio. La corrispondenza tra nominativo del paziente e il Codice univoco sarà registrata su file Excel separato in uso solo allo Sperimentatore principale.

Il responsabile dei dati e della loro pseudonimizzazione è lo Sperimentatore principale.

6.3 Controllo degli accessi logici

L'accesso alla eCRF tramite l'applicativo REDCap è controllato tramite autenticazione con password e, in alcuni casi, anche con codice di verifica.
Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore.

6.4 Tracciabilità

La Piattaforma REDCap garantisce la tracciabilità delle variazioni al progetto, tra cui Esportazione dei Dati, Variazione ai Campi e alla Struttura della Scheda di Raccolta Dati, Variazione nei Dati, Creazione/Aggiornamento/Cancellazione di Utenti, Creazione/Aggiornamento/Cancellazione di Record, Record Locking & e-signature.

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

La Piattaforma REDCap viene aggiornata all'ultima versione rilasciata stabile e sicura disponibile.
Le postazioni di lavoro sono aggiornate regolarmente e protette da sistemi anti-malware.
Le reti dono protette da firewall e strumenti di monitoraggio delle intrusioni.

6.7 Vulnerabilità

La protezione contro le vulnerabilità è garantita attraverso le seguenti attività:

- formazione del personale incaricato al trattamento dei dati
- aggiornamento del sistema almeno annuale
- utilizzo di software e sistemi operativi supportati dal produttore
- sincronizzazione NTP
- piani di risposta agli incidenti

6.8 Backup

Sono presenti:
-Backup giornalieri dei dati e test periodici del sistema di ripristino;
-valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.

6.9 Archiviazione

Le password per l'accesso alla e-CRF vengono custodite su un computer dedicato con accesso riservato, in ufficio del Principal investigator, sito in Farmacia.
I dati vengono conservati nella eCRF fino a 7 anni successivi alla conclusione dello studio.

6.10 Sicurezza dei documenti cartacei

Non è previsto l'utilizzo di documenti cartacei in merito alla gestione dei dati relativi allo studio

6.11 Sicurezza dell'hardware

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

6.12 Gestione postazioni

Il Titolare gestisce le proprie postazioni con XDR.
La gestione delle postazioni comprende la postazione di lavoro dedicata, fisicamente localizzata presso lo studio
dell'Investigatore presso ASST Mantova che viene chiuso a chiave
Al computer dedicato per le attività avranno accesso solo lo Sperimentatore.
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.

L'accesso da rete pubblica è inibito per il computer utilizzato per la gestione dei dati personali. In ogni caso, l'accesso alla intranet aziendale è protetto da Multi-Factor Authentication.

6.13 Manutenzione

La manutenzione del server fisico è demandata al personale IT del Titolare.
Il personale del Fornitore esterno è responsabile del piano di manutenzione ordinaria ed eventualmente evolutiva della Piattaforma REDCap. Il Fornitore esterno esegue aggiornamenti periodici del sistema a versioni compatibili.

6.14 Contratto con il responsabile del trattamento

Il contratto con il responsabile del trattamento contiene opportune istruzioni e disciplina i rispettivi obblighi per assicurare la protezione dei dati personali.

6.15 Controllo degli accessi fisici

Lo studio dove è ubicata la postazione fissa dello Sperimentatore è accessibile solo a quest'ultimo.

Il Titolare ha previsto un protocollo di controllo degli accessi fisici ai locali che ospitano i server, che prevede badge e area videosorvegliata.

6.16 Protezione contro fonti di rischio non umane

Protezione contro fonti di rischio non umane: La presenza di backup giornalieri e periodici evita la perdita di dati.

Eventuali altri controlli legati a guasti, difetti dell'architettura IT, alimentazione, rischi ambientali sono demandati al Titolare.

6.17 Misure di sicurezza in caso di trasferimenti verso Paesi non adeguati

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

6.18 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.

Il DPO dell'ASST di Mantova ha un ruolo di verifica dei trattamenti nei confronti del Titolare del trattamento dati.

6.19 Gestione dei rischi

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

6.20 Integrare la protezione della privacy nei progetti

La fase di progettazione ha tenuto conto dei requisiti di privacy by design.

6.21 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

Gli accordi in essere prevedono la collaborazione di tutti gli Enti coinvolti in caso di incidente.

6.22 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.

6.23 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.

6.24 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.

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 Privacy e DPO.

9. Fase 7: Eventuale consultazione dell'Autorità Garante per la protezione dei dati personali ai sensi dell'art. 36 GDPR

Dato che il trattamento dei dati personali non rientra nei casi previsti dall'art. 110 del D.lgs 196/2003, il Titolare non 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 7) 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:
-Foglio informativo vers 2.0 23.02.2025