Fondazione IRCCS Policlinico San Matteo

Sistema Socio Sanitario
Regione Lombardia

ESTRATTO DELLA VALUTAZIONE DI IMPATTO

DATI DI CONTROLLO DEL DOCUMENTO

Storia del documento				
versione	data	capitolo/paragrafo	modifica apportata	motivo modifica
01	31.07.25	---	Nessuna	Prima versione

1. Informazioni generali

1.1 Titolare del trattamento

La presente DPIA è stata redatta dalla Fondazione S. Matteo, in qualità di Titolare del trattamento ("Titolare del trattamento" o "Fondazione").
Tale ruolo è assunto in quanto la Fondazione è centro partecipante allo studio clinico.
Il Principal Investigator (Responsabile dello studio) è "omissis".

1.2 Contesto di riferimento

Oggetto della presente valutazione d'impatto (Data Protection Impact Assessment – DPIA) è il trattamento dei dati personali dei pazienti che saranno arruolati al fine di condurre:

- Osservazionale ambispettico

Tale studio sarà:

- multicentrico coordinato da altri

1.3 Standard di riferimento per la predisposizione della DPIA

Si rimanda alla procedura aziendale.

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

Si rimanda alla procedura aziendale.

1.5 Team di lavoro

Il presente documento è stato redatto da un team della Sperimentazione con la collaborazione del Team Privacy.

2. Fase 1: Descrizione del trattamento

2.1.1 Il trattamento oggetto della Valutazione di Impatto

Si fa riferimento al protocollo di studio dal titolo "*Studio Nazionale sull'epidemiologia ed efficacia delle terapie nel trattamento della scabbia*" (codice studio SCAB-net) e documentazione studio specifica.

2.1.2 Ruoli e responsabilità collegate al trattamento.

I soggetti che possono intervenire oltre il Titolare del trattamento sono:

- SIDeMaST, Società Italia di Dermatologia Medica, Chirurgica, Estetica e di Malattie Sessualmente Trasmesse in qualità di Promotore e Titolare Autonomo del trattamento;

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.

2.1.2.1.1 Persone fisiche che intervengono nel trattamento:

Le persone fisiche e relativi ruoli saranno elencate nel Delegation Log e includono:

"omissis"

2.1.3 Attività di trattamento

Le attività di trattamento sono finalizzate a valutare i dati epidemiologici (prevalenza, incidenza, etnie e fasce di popolazione affette), i trattamenti più frequentemente utilizzati e gli eventuali fallimenti terapeutici.

2.1.4 Ciclo di vita del trattamento dei dati

I dati verranno estratti dalle cartelle cliniche del paziente e inseriti in forma pseudoanonimizzata nella e-CRF fornita dal Promotore.
I dati verranno mantenuti nella eCRF gestita dal promotore fino al termine dello studio.
Gli stessi saranno successivamente trasferiti su supporto elettronico (chiavetta USB o DVD) che verrà conservato, presso la Fondazione IRCSS Policlinico San Matteo, insieme alla restante documentazione dello studio per almeno 5 anni dopo il termine della sperimentazione.

2.1.5 Finalità e obiettivi del trattamento

Le finalità del trattamento sono:
1) Di ricerca scientifica

2.1.6 Categorie di Interessati

2.1.6.1. Categorie di Interessati: pazienti

2.1.6.2. Numero indicativo degli interessati coinvolti: 30

2.1.7 Dati oggetto di trattamento

- dati anagrafici del caso indice: età, condizioni di immunodepressione o allettamento;
- dati del nucleo familiare del caso indice: numerosità, Stato originario, presenza di casi pediatrici con peso superiore o inferiore ai 15 kg, presenza di barriera linguistica;
- criteri di diagnosi caso indice: clinica e/o dermatoscopica e/o microscopica;
- dati clinici caso indice: aree coinvolte (mani, aree genitali, arti superiori, arti inferiori, tronco, volto, cuoio capelluto), terapie non specifiche precedentemente effettuate;
- giorni di isolamento caso indice (se effettuato);
- dati riguardanti il trattamento: prima terapia specifica anti-acaro effettuata compresa la modalità di somministrazione, giorni dall'esordio di malattia, numero di persone trattate per ogni caso indice, farmaco con cui si è raggiunta la guarigione (se ottenuta) e in quanto tempo;
- dati con la finalità di indagare i fallimenti di terapia: per ogni terapia effettuata saranno compilate le risposte ai quesiti riguardo l'effettuazione del trattamento nei contatti stretti e conviventi, le corrette informazioni riguardo la messa in pratica della bonifica ambientale, numero di cicli di terapia effettuata, se e dopo quanto è stata eseguita la visita di follow up.

Alla visita di follow up, effettuata dopo due settimane dalla fine della terapia e ogni due settimane fino a guarigione, verranno valutati:
- dati riguardanti il trattamento: farmaco con cui si è raggiunta la guarigione (se ottenuta) e in quanto tempo;
- dati con la finalità di indagare i fallimenti di terapia: per ogni terapia effettuata saranno compilate le risposte ai quesiti riguardo l'effettuazione del trattamento nei contatti stretti e conviventi, le corrette informazioni riguardo la messa in pratica della bonifica ambientale, numero di cicli di terapia effettuata, se e dopo quanto è stata eseguita la visita di follow up.

2.2 Dati, processi e beni/strumenti di supporto

Si fa riferimento al protocollo di studio e documentazione studio specifica; in particolare le informazioni sono riportate nel protocollo [paragrafo "Gestione dei dati ed analisi statistica" pag 7-10] e nella informativa per il trattamento dei dati personali studio specifica.

2.2.1 Beni di supporto

- I beni di supporto possono essere raggruppati in:
  - Fonti dei dati:
    - Cartelle cliniche

- Sistema per la gestione eCRF, applicativo web fornito dal Promotore

Database per la conservazione e archiviazione dei dati:

- supporto elettronico (chiavetta USB o DVD)

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

3.1 Proporzionalità e necessità

Lo scopo di miglioramento del processo di cura/prevenzione attraverso la ricerca clinica 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.

3.1.1 Fondamenti legali del trattamento

La base giuridica del trattamento si fonda su:

- Art. 110 d.lgs. 196/2003 (valutazione d'impatto ai sensi dell'art. 35 del GDPR e applicazione di misure a garanzia ai sensi dell'art. 106, comma 2, lettera d).

  Nel caso di specie, per la fase retrospettiva, per alcuni o per la totalità degli interessati non è possibile acquisire il consenso in quanto

  a) non contattabili o deceduti;

Motivi di impossibilità organizzativa:

Come emerge dal protocollo dello studio "...*Potranno essere arruolati anche pazienti in assenza del loro consenso qualora, all'esito della verifica dello stato in vita, risultino deceduti e non aver fornito in precedenza indicazioni contrarie all'uso dei loro dati per scopi di ricerca scientifica, a condizione che il trattamento sia limitato ai dati e alle operazioni strettamente indispensabili e pertinenti per la conduzione dello studio. Nel caso specifico, nell'ambito della realizzazione dello studio, in ottemperanza al regolamento Europeo 679/2016 e al provvedimento del Garante 146/2019, informare i pazienti potenzialmente arruolabili nel presente studio potrebbe risultare impossibile (o implicare uno sforzo sproporzionato). Il non considerare i dati dei soggetti non rintracciabili pregiudica gravemente il conseguimento delle finalità della ricerca qui descritta. La circostanza per cui, 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 non corretta analisi dei relativi risultati. Limitare la popolazione dello Studio a quei pazienti che si recano di persona ai Centri per le visite di routine durante il periodo di arruolamento previsto ridurrebbe notevolmente e sostanzialmente il numero di pazienti coinvolti nello Studio e ciò renderebbe impossibile o comprometterebbe seriamente il raggiungimento dello scopo della ricerca (una dimensione troppo piccola del campione osservato non sarebbe un'evidenza rappresentativa). Inoltre, è stata prevista l'effettuazione della valutazione d'impatto resa nota mediante pubblicazione sui siti del Promotore e dei Centri partecipanti, in sezioni facilmente accessibili e per l'intera durata dello Studio, comunicata al Garante della Privacy nonché al Comitato Etico Territoriale (CET) del Centro Coordinatore di Trento.*

Gli sperimentatori, per ciascuno dei Centri partecipanti, si impegnano a rendere l'informativa agli interessati inclusi nella ricerca in tutti i casi in cui, nel corso dello studio, sia possibile e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo."

- Consenso dell'interessato *ex* art. 6, par.1 lett. a) e art. 9, par. 2, lett. a) del GDPR.

Il consenso è:

- liberamente conferito: la scelta di partecipare allo studio è opzionale e facoltativa, in quanto non l'interessato non subisce conseguenze negative in termini di assistenza sanitaria ricevuta.
- specifico: il consenso viene richiesto per ogni specifica finalità che lo prevede.
- informato: all'interessato sono fornite le opportune informazioni ai sensi degli artt. 12-13 del GDPR.
- inequivocabile: il consenso viene prestato attraverso l'apposizione di firma quale azione positiva dell'utente
- esplicito: la richiesta di consenso è costruita in moda tale da presentare all'utente sia l'opzione di acconsentire sia l'opzione di non acconsentire al trattamento
- revocabile in qualsiasi momento: l'interessato può esercitare il diritto di revoca tramite richiesta effettuata al Titolare del trattamento nella persona del Responsabile dello studio

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

Si rimanda alla procedura aziendale.

3.1.3 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: Principal Investigator e personale del gruppo di ricerca autorizzato.
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.

I dati verranno trattati mediante processo di pseudonimizzazione, ovvero ad ogni soggetto partecipante allo studio verrà assegnato un codice che verrà utilizzato nello studio. La chiave per risalire all'oggetto sarà conosciuta solo dal Principal Investigator e dai ricercatori del gruppo di ricerca autorizzati dal PI.
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.

3.1.4 Durata della conservazione dei dati

I Dati personali dell'interessato saranno conservati per il solo tempo necessario ai fini per cui sono stati raccolti, rispettando i principi di limitazione della conservazione e minimizzazione definiti nell'art. 5 del GDPR.
I Dati saranno custoditi per conformarsi agli obblighi regolatori e perseguire le finalità del trattamento, in conformità coi principi di necessità, minimizzazione e adeguatezza.

Il Titolare del trattamento dichiara che i dati personali dell'interessato oggetto di trattamento saranno conservati per 5 anni dal termine dello studio, come specificato nel protocollo e nell'informativa specifica dello studio.

3.2 Controlli per proteggere i diritti degli interessati

3.2.1 Come sono informati gli interessati circa il trattamento

Si rimanda all'informativa al trattamento dei dati personali studio-specifica consegnata al paziente/pubblicata sul sito internet.

3.2.2 Esercizio dei diritti da parte degli interessati

Si rimanda alla procedura aziendale disponibile sul sito intranet http://intranet.sanmatteo.org/site/home/argomenti/documentazione-privacy/articolo1010755.html

Si rimanda a vademecum per gli utenti disponibile sul sito internet:
https://www.sanmatteo.org/site/home/scheda10871.html

3.2.3 Obbligazioni dei responsabili del trattamento

Non risultano responsabili del trattamento.

3.3 Trasferimenti al di fuori dello SEE

I suoi dati personali non verranno trasferiti fuori dall'Unione Europea da parte di Fondazione IRCCS.

4. Fase 3: Calcolo del livello del rischio

Il livello del rischio e le relative misure di mitigazione viene calcolato utilizzando l'allegato "ADDENDUM CALCOLO DEL RISCHIO".

5. Fase 4: Calcolo del rischio residuo, piano di remediation e parere del DPO

5.1 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.

5.2 Piano di remediation

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

5.3 Opinione del DPO

L'indice di questo documento e relativi contenuti rispecchiano quanto indicato nell'allegato 2 del WP 248 *(Criteri per una valutazione d'impatto sulla protezione dei dati accettabile)* (cfr. Comitato Europeo per la protezione dei dati, Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248rev.01).
Il DPO, consultato dal Titolare in conformità all'art. 35, par. 2, del GDPR in merito alla Valutazione d'impatto ex artt. 35-36 GDPR (cd. DPIA) sulle attività di trattamento relative allo "Studio Nazionale sull'epidemiologia ed efficacia delle terapie nel trattamento della scabbia (SCAB-net)", nello svolgimento dei compiti attribuitigli, ha valutato che**:**

Cfr. parere DPO

Addendum

- **Rispetto dei principi di Privacy by Design e calcolo dell'Impatto**
- Infrastruttura:
  - Computer dedicato
  - Rete: collegamento da Intranet aziendale, e connessione protetta da rete pubblica

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

Calcolo dell'impatto

Si considerano i seguenti livelli di Impatto:

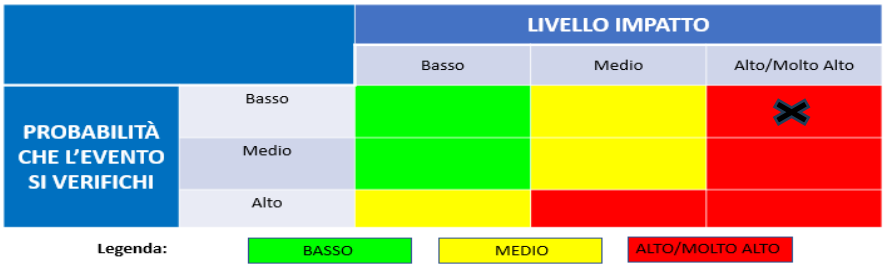
Tabella 1

LIVELLO DI IMPATTO	VALORE	DESCRIZIONE
BASSO	**1**	Gli individui possono andare incontro a **disagi minori**, che supereranno **senza alcun problema** (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
MEDIO	**2**	Gli individui possono andare incontro a **significativi disagi**, che saranno in grado di superare nonostante **alcune difficoltà** (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
ALTO	**3**	Gli individui possono andare incontro a **conseguenze significative**, che dovrebbero essere in grado di superare anche se con **gravi difficoltà** (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
MOLTO ALTO	**4**	Gli individui possono subire **conseguenze significative**, o addirittura irreversibili, **non superabili** (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Il livello d'Impatto deve essere valutato in relazione alle seguenti variabili:

- perdita di riservatezza dei dati;
- perdita d'integrità dei dati;
- perdita di disponibilità dei dati.

- **Calcolo del livello di rischio**



LIVELLO DEL RISCHIO	**ALTO**

- **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.

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 □. In particolare, le misure che maggiormente contribuisco a garantire una maggior tutela della riservatezza sono la pseudonimizzazione e la prevenzione del malware.

- I dati contenuti nella Base Dati sono infatti pseudonimizzati e non permettono quindi di risalire direttamente all'identità degli Interessati.
- I dati della CRF ed i dati identificativi sono soggetti a protezione crittografica.
- Inoltre, gli accessi ai dati personali da parte degli utenti sono permessi solo a seguito di autenticazione attribuendo i permessi sulla base dei ruoli ricoperti.
- Gli accessi fisici sono controllati.
- IL PC sarà tenuto acceso solo durante l'utilizzo effettivo
- Il PC non sarà accessibile via VPN e comunque da remoto: verranno disabilitati/disinstallati i relativi servizi
- 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 □, adottate per mitigare i rischi di perdita d'integrità sono le seguenti:
Prima di tutto vengono eseguiti diversi controlli di qualità sui dati che ne garantiscono l'integrità: controlli di qualità a campione, revisione programmatica delle statistiche descrittive.
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 un backup giornalieri, mensili ed annuali. 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.

- **Fase 4: Misure di mitigazione adottate**
  - **Crittografia - Cifratura**

"omissis"

  - **Pseudonimizzazione**

Vengono implementate tecniche di pseudonimizzazione, al fine di ottenere la separazione tra i dati identificativi del paziente e i dati della CRF in accordo con gli standard di cui al par. 1.4, in particolare l'Opinione 05/2014 del WP29 e la recente NIST SP 800-188.
I dati direttamente identificativi non sono presenti nella CRF essendo sostituiti da una chiave di pseudonimizzazione.
.

- **Controllo degli accessi logici**

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.

- **Tracciabilità**

Vengono tracciati e conservati per un anno i log di eventi di possibile rischio di sicurezza.

- **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

- **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.

- **Vulnerabilità**

Viene assicurata la protezione contro le vulnerabilità attraverso l'attuazione di una manutenzione ordinaria dei sistemi aziendali per l'applicazione di patch di sicurezza.

- **Backup**

Il Titolare è responsabile delle procedure di backup a livello di virtualizzazione o, copia periodica del server database sono impostati backup giornalieri, mensili ed annuali.

- **Archiviazione**

I dati vengono conservati sui server del Titolare fino al termine dello studio. Successivamente tutti i dati verranno salvati su supporto elettronico che verrà conservato, in locale chiuso, insieme alla documentazione cartacea dello studio per 5 anni dal termine dello studio stesso.

- **Sicurezza dei documenti cartacei**

I documenti cartacei prodotti dallo studio sono il modulo di consenso informato e i moduli dell'informativa e del consenso al trattamento dei dati personali.

- **Sicurezza dell'hardware**

Il computer sarà su dominio locale e disporrà delle ultime patch di sicurezza, sempre aggiornate e adeguate alle ultime indicazioni di buona pratica.
Sono applicate le opportune configurazioni di sicurezza relative all'hardware.

- **Gestione postazioni**

La gestione delle postazioni comprende la postazione di lavoro dedicata.
Al computer dedicato per le attività avranno accesso solo il Data Manager e il responsabile scientifico del progetto.
Il computer resterà acceso solo durante il suo utilizzo.

- **Manutenzione**

Per la parte di infrastruttura, la manutenzione del server fisico è demandata al personale IT del Titolare. In particolare, per parti impiantistiche sono previsti contatti di manutenzione ordinaria e straordinaria con outsourcer specifici, mentre per la parte di apparati e sistemi di elaborazione, una volta scaduta la garanzia, sono sottoscritti appositi contratti di manutenzione.
Per la postazione utilizzata, verrà disabilitata la possibilità di accesso VPN.

- **Contratto con il responsabile del trattamento**

Non risultano responsabili del trattamento.

- **Controllo degli accessi fisici**

Lo studio dove è ubicata la postazione fissa utilizzata è accessibile solo a personale autorizzato.

- **Protezione contro fonti di rischio non umane**

Protezione contro fonti di rischio non umane: La presenza di backup giornalieri, mensili ed annuali.
Eventuali altri controlli legati a guasti, difetti dell'architettura IT, alimentazione, rischi ambientali sono demandati al Titolare.

- **Misure di sicurezza in caso di trasferimenti verso Paesi non adeguati**

Non sono previsti trasferimenti al di fuori dello Spazio Economico Europeo da parte di Fondazione IRCCS.

- **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.
La Fondazione, al fine di garantire la conformità alla normativa in materia di protezione dei dati personali, ha provveduto a costituire un Gruppo Operativo Privacy e a nominare il DPO.
Il DPO della Fondazione ha un ruolo di verifica dei trattamenti nei confronti del Titolare del trattamento dati.

- **Gestione dei rischi**

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

- **Integrare la protezione della privacy nei progetti**

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

- **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.

- **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.
Viene effettuata attività di formazione per il personale che a vario titolo è coinvolto nel trattamento dei dati (dipendenti, tirocinanti etc). Sono pianificati annualmente gli interventi formativi.

- **Gestione dei terzi che accedono ai dati**

Il Promotore potrà accedere solo ai dati pseudonimizzati dello studio.

- **Vigilanza sulla protezione dei dati**

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

3 Opinione del DPO

CFR (parere DPO)

4 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.