VAL/UTAZIONE DI IMPATTO

STUDIO DAL TITOLO *INTERCETTARE PRECOCEMENTE LE GAMMOPATIE MONOCLONALI IGM*

Versione:	***1.0 data 09/11/2026***

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 il promotore dello studio, avendone determinato finalità e mezzi di trattamento.

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:

- uno studio osservazionale ambispettico

Tale studio sarà:

- multicentrico coordinato dalla Fondazione

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 *Intercettare precocemente le gammopatie monoclonali IgM* e documentazione studio specifica

2.1.2 Ruoli e responsabilità collegate al trattamento.

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

- *Sponsor (Fondazione IRCCS Policlinico San Matteo, Viale C. Golgi 191 27100, Pavia)* in qualità di Promotore e Titolare Autonomo del trattamento;
- *Fornitore della eCRF (Biomeris quando si utilizza Redcap) (in qualità di Responsabile del trattamento per le attività di assistenza/manutenzione IT relative al presente progetto di ricerca per conto della Fondazione IRCCS)*

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.

2.1.3 Attività di trattamento

Le attività di trattamento sono finalizzate a valutare la fattibilità e l'efficacia di uno screening basato su biomarcatori per la diagnosi precoce di IgM-Al o di altre IgM-MGCS in soggetti a rischio effetti da IgM-MGUS o WM asintomatica.

2.1.4 Ciclo di vita del trattamento dei dati

I dati vengono estratti dalle cartelle cliniche cartacee dei pazienti ed inseriti nella eCRF fornita dalla Fondazione IRCCS Policlinico San Matteo. I dati inseriti sono pseudonomizzati.

2.1.5 Finalità e obiettivi del trattamento

Le finalità del trattamento sono:

1) Di ricerca scientifica
2) Finalità di ricerca scientifica e statistica volta alla tutela della salute dell'Interessato, di terzi o della collettività in campo medico, biomedico ed epidemiologico" in caso di trattamento di dati genetici;
3) Conservazione prolungata dei campioni biologici e dati personali - NON NECESSARIA ai fini della partecipazione allo studio e al suo svolgimento - per le future attività di ricerca, per le quali sarà elaborata apposita informativa e formula di consenso";

2.1.6 Categorie di Interessati

2.1.6.1. Categorie di Interessati: pazienti adulti affetti da IgM-MGUS, WM asintomatica o sintomatica, IgM-AL o altre IgM-MGCS associate a una componente monoclonale IgM, naïve al trattamento al momento dell'arruolamento.

2.1.6.2. Numero indicativo degli interessati coinvolti: la Fondazione ne dichiara 250 pazienti

2.1.7 Dati oggetto di trattamento

2.1.7.1. Dati comuni trattati:

- Dati anagrafici: nome, cognome, età, sesso
- Dati di contatto: indirizzo mail, telefono

2.1.7.2. Dati appartenenti alle categorie particolari trattati:

- dati genetici
- dati relativi alla salute
- campioni biologici
- Dati contenuti nella CRF (elenco sintetico): identificazione, eleggibilità, caratteristiche della gammopatia clonale, biomarcatori, coinvolgimento cardiaco, renale, epatico, neurologico, tessuti molli, osseo, diagnosi di amiloidosi, stadiazione, terapia, risposta ematologia-d'organo, malattia minima residua, follow up, analisi molecolari e biomarcatori esplorativi);

2.1.7.3. Raccolta e gestione dei campioni biologici: i campioni che verranno raccolti saranno analizzati dalla Fondazione (SC Ematologia 1 e SC Centro Amiloidosi Sistematiche e Malattie ad Alta Complessità e archiviati nel padiglione 14 della Fondazione, SC Ematologia 1). I campioni saranno contrassegnati con un codice di partecipazione allo studio e non conteranno altre informazioni identificative del paziente.

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

2.2.1 Beni di supporto

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

Software per la gestione della CRF (e-CRF):

- REDCap (Version 14.0.15 - © 2024 Vanderbilt University). *(in presenza di Redcap della Fondazione)*

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 bis, quarto comma, 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, lo Studio è promosso da una IRCCS e, pertanto, non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca.

- 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")

Per l'esecuzione del trattamento, il Titolare del trattamento raccoglierà solo i dati adeguati, rilevanti e limitati a quanto necessario per il conseguimento delle finalità del trattamento. Si rimanda a tal fine alla procedura aziendale e al Protocollo di studio.

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 10 anni , 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.html alla sezione privacy

Si rimanda a vademecum per gli utenti disponibile sul sito internet: https://www.sanmatteo.org alla sezione privacy

3.2.3 Obbligazioni dei responsabili del trattamento

(Biomeris srl) è stato individuato quale responsabile del trattamento *ex* art. 28 del GDPR con apposito atto di nomina, in ragione della fornitura della piattaforma RedCap.

3.3 Trasferimenti al di fuori dello SEE

I suoi dati personali non verranno trasferiti fuori dall'Unione Europea.

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 clinico – *Intercettare precocemente le gammopatie monoclonali IgM*", nello svolgimento dei compiti attribuitigli, ha valutato che**:**

Cfr. parere DPO

VALUTAZIONE DI IMPATTO

INDICE

1 Rispetto dei principi di Privacy by Design e calcolo dell'Impatto

1.1 Software per la gestione della CRF (e-CRF) e Infrastruttura

- REDCap (Version 14.0.15 - © 2024 Vanderbilt University).

- Infrastruttura:
  - Computer dedicato

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.

LIVELLO DEL RISCHIO	**ALTO**

2 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 del PC che permettendo 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 la probabilità di accadimento delle minacce?

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.

- 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.
- Inoltre, gli accessi ai dati personali da parte degli utenti finali della Piattaforma sono permessi solo a seguito di autenticazione a due fattori (TFA – Two Factor Authentication) attribuendo i permessi sulla base dei ruoli ricoperti.
- Gli accessi fisici sono controllati e le postazioni gestite.
- Viene erogata regolare formazione agli autorizzati al trattamento.
- (omissis)

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 dati che ne garantiscono l'integrità: controlli di qualità a campione tramite il modulo 'Data Quality Rules' previsto nella piattaforma REDCap.
- (omissis).
- Gli accessi fisici sono controllati e le postazioni gestite.
- (omissis)

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 giornaliero con retention (omissis)

3. Misure di mitigazione adottate

3.1 Crittografia – Cifratura

Vengono implementate le seguenti tecniche di cifratura dei dati personali:
In transito:

- il protocollo di trasporto dei dati tra application server e database è crittografato HTTPS (HyperText Transfer Protocol over Secure Socket Layer) con certificato x509 (Direct Trust mutual Transport-Level Security ovvero mutua autenticazione con scambio di certificat) e protocollo TLS 1.2
- La sequenza dei messaggi di richiesta/risposta avviene dopo aver instaurato il canale di trasmissione sicuro.
- I dati trasferiti durante le attività di backup sono trasmessi su canali sicuri.

At Rest:

- Sono applicate le adeguate misure di crittografia sul dato a riposo. Nello specifico a riposo il database viene crittografato con algoritmo AES a 128 bit.

3.2 Pseudonimizzazione

Vengono implementate tecniche di pseudonimizzazione, al fine di 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 costituito da un codice alfanumerico progressivo, contestualmente all'ingresso del paziente nello studio e alla firma del consenso informato (GCP E6(R2)), tale passaggio è fondamentale per permettere allo Staff dello studio di compilare la eCRF con i dati relativi al paziente corrispondente ed eseguire periodicamente le "Data Quality Rules" (par. 3.1.2.5 Fase di Data Quality) tramite la piattaforma. Lo Sperimentatore Principale e lo Study Coordinator avranno accesso alla corrispondenza tra tale ID e l'identificativo univoco ospedaliero del paziente, che verrà conservato in un file separato (Subject Enrolment Log) conservato in uno storage protetto presso la Fondazione e gestito da personale autorizzato dal Titolare.
Non viene, inoltre, riportata la data di nascita del paziente essendo stata sostituita con l'età al momento della procedura. Sono invece presenti date puntuali collegate ai diversi episodi, in quanto ritenute fondamentali per le analisi oggetto dello studio. Tali date potrebbero costituire insieme ad altri identificativi indiretti una potenziale individuazione del paziente solo tramite accesso alla documentazione clinica originaria, salvo una puntuale conoscenza personale del paziente da parte dell'eventuale attaccante che potrebbe comportare l'inferenza di ulteriori informazioni sanitarie. Si ritiene, tuttavia, questo rischio contenuto in quanto in fase di export dei dati verrà applicato uno shift casuale (di un valore compreso tra 0 e 364) alle date puntuali.
Il responsabile dei dati e della loro pseudonimizzazione è lo sperimentatore principale.

3.3 Controllo degli accessi logici

L'accesso alla eCRF tramite l'applicativo REDCap è controllato tramite MFA: password e codice di verifica (inviato via mail o reperibile tramite Google/Microsoft Authenticator).
Il file relativo alle corrispondenze e la eCRF in REDCap saranno protetti tramite password (con scadenza ogni 60 giorni) differenti con criteri di robustezza quali:

- Lunghezza minima 9 caratteri
- Lettere maiuscole e minuscole
- Cifre di base 10 (da 0 a 9)
- Caratteri alfanumerici: !@#$%^&*()/_+|~=',-*+:\";?. (esclusi ><\)

La sicurezza degli accessi nella componente server che permette l'accesso ai dati coinvolge l'autorizzazione che viene gestita sempre all'interno della Piattaforma utilizzando l'interfaccia web REDCap. Viene implementato un modello RBAC (Role-Based Access Control) dove i privilegi, relativi alle singole funzioni erogabili dal sistema rispetto ad ogni dataset in esso contenuto, vengono collegati a specifici ruoli che, in una fase successiva, sono assegnati agli utenti.
Il personale afferente alla SSD Biostatistica e Clinical Trial Center della Fondazione assegna le utenze individuali in REDCap al personale, autorizzato dal Principal Investigator, che si occuperà della creazione della eCRF e dell'inserimento dei dati.

3.4 Tracciabilità

La Piattaforma REDCap è dotata di una applicazione interna denominata "Logging", tramite cui vengono registrate tutte le 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.

Tali informazioni verranno conservate per 2 anni sui server del Titolare.

3.5 Minimizzazione dei dati

Verranno raccolti tutti e soli i dati necessari per rispondere ai quesiti dello studio.

- 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

3.6 Lotta contro il malware

La Piattaforma REDCap viene aggiornata all'ultima versione rilasciata stabile e sicura disponibile. Tale aggiornamento è demandato ad un Fornitore esterno.

3.7 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.
Inoltre, 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
- vapt annuali
- piattaforma di gestione centralizzata delle vulnerabilità

3.8 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 e retention.

3.9 Archiviazione

I dati vengono conservati sui server del Titolare fino a 10 anni successivi alla loro raccolta nella eCRF. (omissis)

3.10 Sicurezza dei documenti cartacei

Le configurazioni di sicurezza relative all'hardware su ci è installata la Piattaforma sono demandate al personale IT del Titolare.
I documenti cartacei prodotti dallo studio sono: documentazione relativa allo studio: il Protocollo, la sinossi, la CRF, il consenso sanitario ecc., i moduli dell'informativa e del consenso al trattamento dei dati personali ai sensi dell'art. 13 del Regolamento UE 679/2016- GDPR, cartelle ambulatoriali.
Essi sono conservati in armadi chiusi a chiave ed in locali dotati di misure antincendio (omissis)

3.11 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.

3.12 Gestione postazioni

Il Titolare gestisce le proprie postazioni con XDR.
La gestione delle postazioni comprende la postazione di lavoro dedicata, fisicamente localizzata presso la SC. Ematologia 1, studio del PI Marzia Varettoni che viene chiuso a chiave.
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.

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 (Cisco Duo).

3.13 Manutenzione

La manutenzione del server fisico è demandata al personale IT del Titolare e al fornitore appositamente incaricato e nominato e sono applicate le patch e gli aggiornamenti periodici (O.S.) rilasciati dalla casa madre. Il personale del Fornitore esterno è responsabile del piano di manutenzione ordinaria ed eventualmente evolutiva della Piattaforma REDCap. Il Fornitore esterno esegue un aggiornamento annuale del sistema a versioni compatibili.

3.14 Contratto con il responsabile del trattamento

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

3.15 Controllo degli accessi fisici

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

3.16 Protezione contro fonti di rischio non umane

Protezione contro fonti di rischio non umane: La presenza di backup giornalieri, mensili ed annuali e retention di almeno 7 gg su server separati evita la perdita di dati.
Eventuali altri controlli legati a guasti, difetti dell'architettura IT, alimentazione, rischi ambientali sono demandati al Titolare.

3.17 Politica di tutela della privacy

Le politiche privacy del Titolare del trattamento e dei responsabili del trattamento, relative alla propria organizzazione, sono conformi al GDPR.
Il DPO di Fondazione IRCCS Policlinico San Matteo ha un ruolo di verifica dei trattamenti nei confronti del Titolare del trattamento dati
È stato emesso un Organigramma Privacy che definisce i ruoli all'interno dell'azienda e sono state definite le procedure per la gestione dei diritti degli interessati e la gestione delle violazioni di dati personali.

3.18 Gestione dei rischi

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

3.19 Integrare la protezione della privacy nei progetti

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

3.20 Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Titolare ha adottato una procedura per la gestione degli incidenti di sicurezza.
Gli accordi in essere prevedono la collaborazione di tutti gli Enti coinvolti in caso di incidente.

3.21 Gestione del personale

Il Titolare ha provveduto ad autorizzare il personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati).
Inoltre, ha provveduto a comunicare la disponibilità di procedure privacy al personale a vario titolo coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Le Procedure sono reperibili sulla intranet aziendale.
Sono state svolte attività di formazione (formazione residenziale e corsi FAD) per tutto il personale che a vario titolo è coinvolto nel trattamento dei dati (dipendenti, tirocinanti e somministrati). Inoltre pianifica

annualmente gli interventi formativi.

3.22 Gestione dei terzi che accedono ai dati

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

3.23 Vigilanza sulla protezione dei dati

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

7 Opinione del DPO

CFR (parere DPO)

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.