VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI AI SENSI DELL'ART. 35 DEL GDPR PER LO STUDIO DAL TITOLO:

"Valutazione dell'efficacia e della tollerabilità di ruxolitinib topico nella real-life per la terapia della vitiligine non segmentale"

ACRONIMO: RE-VIT-RUX

Predisposizione: Dott.ssa Federica Ravetti

Valutazione: Avv. Margherita Clerici, Referente privacy

Validazione: Prof.ssa Silvana Castaldi, Data Protection Officer

Stato: Adottata il 30 dicembre 2025

Versione: 1

Sommario

1. Premessa

La presente valutazione d'impatto ("*Data Protection Impact Assessment*"- "**DPIA**") è stata realizzata 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***").*

2. Valutazione della necessità di redigere una DPIA

Ai sensi dell'art. 35, comma 1, del GDPR, il Titolare del trattamento deve effettuare una valutazione dell'impatto sulla protezione dei dati personali degli interessati prima di avviare un trattamento quando - considerati la natura, l'oggetto, il contesto e le finalità – quest'ultimo può presentare un rischio elevato per i diritti e le libertà degli interessati. Allo scopo di supportare il Titolare nella valutazione se un trattamento comporti un rischio elevato e, quindi, sia necessario effettuare una DPIA, il Gruppo Art. 29 (ora "**EDPB**") nelle Linee Guida suggerisce di prendere in esame nove criteri. La predetta valutazione si renderà necessaria ove il trattamento soddisfi almeno due dei nove criteri ivi elencati. Anche l'EDPB, negli esempi contenuti nella tabella presente all'interno delle Linee Guida, valuta come potenzialmente rischioso per i diritti e le libertà dei soggetti arruolati, il trattamento relativo alla conservazione per finalità di archiviazione di dati personali sensibili relativi a interessati coinvolti in progetti di ricerca o sperimentazioni cliniche, anche se pseudonimizzati. Inoltre, ai sensi dell'art. 35.1 del GDPR, una singola valutazione d'impatto può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Sulla base del citato quadro normativo, la Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico (Promotore) e i Centri partecipanti elencati nel presente documento, ciascuno per gli ambiti di propria competenza, sono Titolari autonomi del trattamento.

La Fondazione ha predisposto la presente DPIA nella quale sono analizzati i rischi connessi al trattamento dei Dati Personali raccolti nell'ambito dello studio dal titolo "**Valutazione dell'efficacia e della tollerabilità di ruxolitinib topico nella real-life per la terapia della vitiligine non segmentale".**

3. Definizioni

Codice: Decreto legislativo 196/2003 e s.m.i, Codice in materia di protezione dei dati personali

Dati Personali: dati personali, così come definiti dall'art. 4.1) del Regolamento UE 2016/679 ("**GDPR**"), trattati in forma pseudonimizzata dalla Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico ("**Fondazione**") per la conduzione dello studio dal titolo**: "Valutazione dell'efficacia e della tollerabilità di ruxolitinib topico nella real-life per la terapia della vitiligine non segmentale".**

Database Dati Personali: l'insieme delle eCRF specifiche dello Studio salvate sulla piattaforma REDCap.

Piattaforma: RedCap (Research Electronic Data Capture). Il Consorzio REDCap è composto da >1000 partner istituzionali in tutto il mondo (enti di ricerca, università, ministeri etc). Il consorzio supporta un'applicazione web sicura (REDCap) progettata esclusivamente per supportare l'acquisizione di dati per studi di ricerca. L'applicazione REDCap consente agli utenti di creare e gestire banche dati on-line in modo rapido e sicuro,

ed è attualmente in uso per più di 110.000 progetti con circa 150.000 utenti che coprono numerose aree di interesse di ricerca in tutto il consorzio.

Studio: studio no profit, multicentrico, osservazionale, retrospettivo, farmacologico.

Interessati: i soggetti arruolati nello Studio presso la Fondazione a cui i Dati Personali si riferiscono.

- Numero di soggetti previsti per lo studio: 200

Ricercatori e altro personale del Titolare coinvolti nello studio.

Centri Partecipanti: si intendono i centri clinici che hanno aderito allo studio e partecipano in qualità di centri arruolanti. Tra tali centri si annoverano:

1. SC Dermatologia, Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico di Milano, Italia. (Responsabile: Prof. Angelo Marzano)

2. Section of Dermatology, Dipartimento di Medicina Clinica e Chirurgia, Università degli Studi di Napoli "Federico II" – Napoli (Responsabile: Maddalena Napolitano)

3. Dipartimento della Salute della Donna e del Bambino, Università di Padova (Responsabile: Anna Belloni Fortina)

4. Clinica Dermatologica, Policlinico di Bari "Aldo Moro"; Dipartimento Scienze Biomediche e Oncologia Umana, Università di Bari Aldo Moro – Bari (Responsabile: Caterina Foti)

5. Azienda Ospedaliera – Università di Bari "Aldo Moro", Policlinico di Bari – Bari (Responsabile: Eustachio Nettis)

6. Dermatology Unit, IRCCS Humanitas Research Hospital & Humanitas University – Rozzano (MI) (Responsabile: Alessandra Narcisi)

7. Clinica Dermatologica, AOU "Città della Salute e della Scienza di Torino"; Dipartimento di Scienze Mediche, Università degli Studi di Torino – Torino (Responsabile: Simone Ribero)

8. U.O. Dermatologia, ASST Valle Olona – Ospedale Sant'Antonio Abate – Gallarate (VA) (Responsabile: Serena Giacalone)

9. Dipartimento Scienze Mediche e Chirurgiche, Policlinico Universitario Agostino Gemelli – IRCCS, Università Cattolica del Sacro Cuore – Roma (Responsabile: Ketty Peris)

10. Università Vita-Salute San Raffaele & IRCCS Ospedale San Raffaele – Milano (Responsabile: Franco Rongioletti)

11. ASST Papa Giovanni XXIII – Bergamo (Responsabile: Paolo Sena)

12. IRCCS Ospedale San Raffaele & Università Vita-Salute San Raffaele – Milano (Responsabile: Santo Raffaele Mercuri)

13. U.O. Dermatologia, Azienda Ospedaliero-Universitaria Sant'Anna e Università degli Studi di Ferrara – Ferrara (Responsabile: Alessandro Borghi)

14. Dipartimento di Dermatologia, Università degli Studi e Ospedale Universitario di Trieste – Trieste (Responsabile: Iris Zalaudek)

15. Università Unicamillus & Istituto Dermatologico San Gallicano IRCCS "IDI" – Roma (Responsabile: Mauro Picardo)

16. Dipartimento di Medicina e Scienze dell'Invecchiamento, Università "G. d'Annunzio" – Chieti-Pescara (Responsabile: Paolo Amerio)

17. Sezione di Dermatologia, Azienda Ospedaliero-Universitaria Integrata di Verona & Università di Verona – Verona (Responsabile: Francesco Bellinato)

18. SOS Dermatologia Speciale Medica, Azienda USL Toscana Centro – Firenze (Responsabile: Emiliano Antiga)

19. UOC Dermatologia, Fondazione IRCCS Policlinico San Matteo; Università degli Studi di Pavia – Pavia (Responsabile: Carlo Francesco Tomasini)

Per quanto non espressamente definito nel presente documento si rinvia alle definizioni contenute nell'art. 4 del GDPR.

4. Descrizione del trattamento

4.1 Finalità del trattamento e contesto dello studio

(presentare sinteticamente il trattamento: denominazione, finalità, risultati attesi, contesto di utilizzo, ...)

Acronimo: RE-VIT-RUX

Promotore: Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico

Centro coordinatore: SC Dermatologia

Sperimentatore principale: Prof. Angelo Valerio Marzano

Oggetto del presente atto di DPIA è il trattamento dei dati che avverrà nell'ambito dello Studio.

La vitiligine non segmentale è una patologia autoimmune cronica caratterizzata dalla perdita di melanociti e presenza di macchie depigmentate. Ruxolitinib crema 1,5% è l'unica terapia approvata per questa condizione, con dimostrazione di efficacia nei trial TRuE-V1/V2. Tuttavia, mancano dati real-life estesi sull'efficacia e la tollerabilità a lungo termine in Italia.

OBIETTIVI DELLO STUDIO

<u>Obiettivo primario</u>

Valutare l'efficacia real-life dell'applicazione di ruxolitinib topico sul viso, in termini di miglioramento del F-VASI a 24 settimane.

Obiettivi secondari

1. Valutare la risposta al trattamento sul viso mediante F-VESplus a 24 settimane.
2. Valutare l'estensione e ripigmentazione delle lesioni corporee mediante VASI e VESplus a 12 e 52 settimane.
3. Valutare la percezione del miglioramento da parte dei pazienti con il VNS a 12, 24 e 52 settimane.
4. Valutare la qualità della vita tramite VitiQoL, DLQI, PHQ-9 e GAD-7 a 12, 24 e 52 settimane.
5. Valutare la tollerabilità e la frequenza di eventi avversi nel lungo termine.
6. Valutare i predittori di risposta terapeutica a 12, 24 e 52 settimane.

Endpoint primario:

Miglioramento del F-VASI a 24 settimane

Endpoint secondari:

- Miglioramento del F-VESplus a 24 settimane.

- Modifica del VASI e del VESplus a 12 e 52 settimane.

- VNS a 12, 24 e 52 settimane.

- VitiQoL, DLQI, PHQ-9 e GAD-7 a 12, 24 e 52 settimane.

- Frequenza e tipo di eventi avversi.

- Analisi dei predittori di risposta terapeutica (età, sesso, attività della malattia, fototipo del paziente, durata della malattia, sedi interessate) a 12, 24 e 52 settimane.

4.2 Responsabilità connesse al trattamento

(Descrivere le responsabilità dei soggetti coinvolti: Titolare del trattamento, eventuali responsabili e contitolari)

La Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico, con sede legale a Milano in Via Francesco Sforza 28, agisce come Titolare del Trattamento, per la raccolta, la conservazione, la pseudonimizzazione o anonimizzazione.

Parimenti, in virtù del suo ruolo di Promotore dello studio clinico, è Titolare autonomo del trattamento dei dati necessario alla conduzione delle attività oggetto di studio.

I singoli centri partecipanti agiranno in qualità di Titolari autonomi del trattamento.

4.3 Standard applicabili al trattamento dei dati

(Elencare gli Standard rilevanti applicabili al trattamento in quanto utili o obbligatori, specialmente i codici di condotta approvati e le certificazioni in materia di protezione dati)

I dati verranno utilizzati nel rispetto delle Good Clinical Practice ("GCP") ossia lo standard internazionale di etica e qualità scientifica per progettare, condurre, registrare e relazionare gli studi clinici che coinvolgano soggetti umani (D.M. 15 luglio del 1997 e ss.mm.ii.). L'aderenza alle GCP garantisce pubblicamente non solo la tutela dei diritti, della sicurezza e del benessere dei soggetti che partecipano allo studio, in conformità con i princìpi stabiliti dalla Dichiarazione di Helsinki dell'Associazione medica mondiale del giugno 1964, ma anche l'attendibilità dei dati relativi allo studio clinico. Nella conduzione dello Studio sono, inoltre, rispettate le prescrizioni delle Linee guida sulla sperimentazione clinica adottate dal Garante per la protezione dei dati personali con Provvedimento 24 luglio 2008 n. 52 e delle Regole Deontologiche (Provvedimento 19 dicembre 2018 n. 515), il Provvedimento n. 146 del 5 giugno 2019, nonché le Linee Guida EDPB 01/2025 in merito alla Pseudonimizzazione.

Il trattamento dei Dati Personali avverrà in modo lecito, corretto e trasparente per finalità determinate, esplicite e legittime, nonché mediante strumenti informatici e cartacei e nel rispetto di leggi, regolamenti e provvedimenti applicabili, adottati anche dall'Autorità Garante per la Protezione dei dati personali, in particolare nell'ambito del trattamento delle categorie particolari di dati personali, ai sensi dell'art. 9 del GDPR.

Tutte le operazioni nell'ambito dello studio saranno effettuate solo da personale debitamente istruito e autorizzato dal Titolare (Fondazione) o dai propri delegati e si svolgeranno nel rispetto del segreto professionale e dei principi di correttezza, liceità e trasparenza, nel rispetto della normativa vigente.

4.4 Categorie di interessati

- Pazienti che presentano le seguenti caratteristiche di inclusione:

Criteri di inclusione:

- Età ≥12 anni
- Diagnosi di vitiligine non segmentale
- Trattamento con ruxolitinib crema 1,5% per almeno 6 mesi
- Disponibilità di dati clinici sufficienti per la valutazione

Saranno esclusi dallo studio i pazienti che non soddisfano i criteri sopra riportati e che presentano i seguenti criteri:

- Mancanza di dati sufficienti al follow-up

- Ricercatori e altro personale del Titolare coinvolti nello studio

4.5 Categorie di dati trattati

Variabili

- *Variabili demografiche (età, sesso, fototipo)*
- *Caratteristiche cliniche della vitiligine (durata, sede, estensione)*
- *F-VASI, F-VESplus, VASI, VESplus*

- *VNS, VitiQoL, DLQI, PHQ-9, GAD-7*
- *Eventi avversi*
- *Aderenza e persistenza alla terapia*

4.6 Accesso ai dati

Soggetti che accedono ai dati personali

Ad ogni partecipante, al momento dell'arruolamento, verrà assegnato un codice univoco. L'identificazione dei dati avverrà in maniera cale che le persone che accedono al database non potranno risalire in alcun modo all'identità dei soggetti. Solo gli sperimentatori locali potranno risalire all'identità dei soggetti arruolati.

Per garantire un adeguato controllo sulla qualità dello studio, lo sperimentatore consentirà, se richiesto, di accedere direttamente a tutta la documentazione pertinente e dedicare parte del suo tempo per discutere i risultati dello studio. Inoltre, le Autorità Regolatorie possono eseguire ispezioni. In questo caso. lo sperimentatore deve autorizzare all'ispettore l'accesso diretto a tutta la documentazione pertinente, e dedicare parte del suo tempo e del suo personale all'ispettore stesso per discutere i risultati del monitoraggio ed eventuali altri aspetti dello studio. Se applicabile, per tutti gli inserimenti manuali dei dati è la richiesta la presenza di due operatori per evitare eventuali errori.

Piano di divulgazione e comunicazione dei risultati

Il responsabile scientifico dello studio si impegnerà nella stesura di un rapporto finale ed a rendere pubblici i risultati al termine dello studio. I dati saranno resi pubblici in modo anonimo e presentati per quanto richiesto in modalità aggregata.

4.7 Modalità di raccolta e conservazione dei dati: strumento e tecnologie utilizzati

I dati necessari per lo studio verranno registrati in una apposita eCRF in un Data Management System secondo la normativa nazionale, fornito dalla Direzione Scientifica della Fondazione. La piattaforma utilizzata sarà RedCap (Research Electronic Data Capture). Il Consorzio REDCap è composto da >1000 partner istituzionali in tutto il mondo (enti di ricerca, università, ministeri etc). Il consorzio supporta un'applicazione web sicura (REDCap) progettata esclusivamente per supportare l'acquisizione di dati per studi di ricerca. L'applicazione REDCap consente agli utenti di creare e gestire banche dati on-line in modo rapido e sicuro, ed è attualmente in uso per più di 110.000 progetti con circa 150.000 utenti che coprono numerose aree di interesse di ricerca in tutto il consorzio. Tramite REDCap, per questo studio verranno messi in atto: a) identificazione a livello di utente, con restrizioni specifiche in base al ruolo nello studio b) validazione e controllo dell'integrità dei dati in tempo reale c) de-identificazione dei pazienti prima dell'esportazione dei dati d) archiviazione centralizzata dei dati con backup giornaliero, un server sicuro all'interno della struttura informatica della Fondazione.

5. Principi fondamentali

5.1 Basi giuridiche che rendono lecito il trattamento dei dati

Ai sensi dell'art. 110 bis IV comma del Codice della Privacy, non costituisce trattamento ulteriore il trattamento dei dati personali raccolti per attività clinica a fini di ricerca da parte di IRCCS in virtù del carattere strumentale dell'attività di assistenza sanitaria rispetto alla ricerca dei predetti istituti. Come confermato dal Garante per la protezione dei dati personali, la disposizione trova applicazione in relazione a ogni tipo di ricerca medica, biomedica, di natura retrospettiva e prospettica, compresi gli studi multicentrici con la partecipazione di enti che non godono di tale riconoscimento.

5.2 Periodo di conservazione dei dati

I dati vengono conservati per la durata dello studio stimata in 10 anni dalla sua approvazione e comunque per un periodo non superiore a 10 anni, in conformità a quanto stabilito dal Regolamento UE 2014/536.

6. Misure a tutela degli interessati

6.1 Modalità di informazione degli interessati

Poiché verranno trattati Dati Personali di pazienti raccolti durante la normale attività di pratica clinica, in virtù dell'art. 110 bis IV comma del Codice (che esclude l'obbligo per gli istituti di ricovero e cura di chiedere un consenso agli interessati per i dati raccolti durante l'attività assistenziale in quanto l'attività di ricerca successiva non costituisce ulteriore trattamento in virtù della stretta correlazione dell'attività assistenziale con quella di ricerca) non verrà richiesto alcun consenso ai soggetti interessati.

In virtù dei chiarimenti dettati dal Garante per la protezione dei dati personali nel documento relativo a "presupposti giuridici e principali adempimenti per il trattamento dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca" sarà possibile non richiedere il consenso anche per gli altri partecipanti che non hanno natura di IRCCS.

Al fine di assolvere all'obbligo informativo dei pazienti, ai sensi dell'art. 14 del Regolamento, sarà comunque predisposta e pubblicata sul sito web di Fondazione e dei Centri partecipanti l'informativa al trattamento dei dati personali.

6.2 Modalità di esercizio dei diritti da parte degli interessati

I soggetti interessati potranno esercitare i loro diritti scrivendo:
- all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy della Fondazione: dpo@policlinico.mi.it
- direttamente presso il PI e la sua equipe (ciò avviene più frequentemente rispetto all'utilizzo della posta elettronica).

Il diritto alla portabilità non è applicabile per tale attività di trattamento. La Fondazione ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

7. Rischi

7.1 Misure tecniche esistenti o pianificate

Accesso illegittimo ai dati

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

Perdita di riservatezza e controllo sui dati presenti all'interno delle cartelle cliniche

Diffusione non autorizzata

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Ingresso di personale non autorizzato in locali in cui sono custoditi i documenti contenenti dati personali relativi allo studio

Utilizzo inappropriato delle password di accesso al pc e alla piattaforma di raccolta dati

Sottrazione delle password di accesso da parte di un terzo

Quali sono le fonti di rischio?

Fonti interne: utilizzo inappropriato della piattaforma di raccolta dati, lasciare incustodita la postazione, operatore interno mal istruito o insoddisfatto

Fonti esterne: hacker

Fonti non umane: virus, bug

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Formazione adeguata del personale che interagisce con la piattaforma di raccolta dati, misure anti-intrusive, controllo accessi, politiche di sicurezza informatica e di tutela privacy.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Marginale

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Poco probabile

Modifiche indesiderate dei dati

Quali potrebbe essere gli impatti sugli interessati se il rischio si dovesse concretizzare?

Dati non esatti o non aggiornati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Errore operativo (es mancato salvataggio delle informazioni, errore di inserimenti dati nella piattaforma)

Quali sono le fonti rischio?

Accesso da parte di soggetti non autorizzati; attacco ai sistemi aziendali; personale negligente o privo di adeguata formazione

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Istruzione di soggetti autorizzati al trattamento; formazione; procedure rigorose; politiche di tutela privacy; misure anti-intrusive; politiche di sicurezza informatica; controllo accessi (log). Back-up dei dati; antivirus

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Marginale

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Poco probabile

Perdita dei dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Non si rileva un impatto diretto sugli interessati; tuttavia, la perdita dei dati potrebbe comportare l'impossibilità di proseguire lo studio clinico, causando un impatto indiretto sui soggetti coinvolti.

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

La minaccia principale è quella di una distruzione o cancellazione erronea o volontaria di dati. Le principali minacce possono essere di natura informatica o derivare da un'azione umana.

Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione). Fonti umane esterne (hacker, soggetti senza autorizzazione). Fonti non umane (virus, introduzione di bug)

Quali misure, fra quelle individuare, contribuiscono a mitigare il rischio?

Back-up dei dati, controllo degli accessi, misure anti-intrusive, tracciabilità, politiche di sicurezza informatica

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziale e delle misure pianificate?

Marginale

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Poco probabile

MISURA	ESISTENTI	Note
Nomine responsabili esterni	**N/A**	
Organigramma interno	**x**	
Nomina DPO	**x**	
Informativa	**x**	Verrà pubblicata sul sito di Fondazione
Istruzioni persone autorizzate	**x**	
Backup dei dati	**x**	È previsto un backup giornaliero criptato.
Procedure		
Formazione	**x**	
Controllo degli accessi logici	**x**	Le credenziali di accesso al Database sono studio specifiche e vengono fornite solo agli Sperimentatori principali e al personale autorizzato dalla Fondazione IRCCS nel rispetto dei seguenti principi - la presentazione di documentazione necessaria in caso di richiesta di attivazione utenze; - caratteristiche delle credenziali di accesso; - disattivazione automatica degli account al termine della durata dello Studio; - procedura di verifica periodica degli account attivi e dei ruoli attribuiti; - di cancellazione dei log di accesso alla Piattaforma entro 6 mesi successivi alla fine dello Studio. L'accesso al Database è riservato agli utenti previa autenticazione, l'autenticazione utilizzata è basata su tabella, che utilizza

		l'archiviazione di coppie nome utente/password in una tabella del database. Per motivi di sicurezza, la password nella tabella del database non viene archiviata come testo normale, ma viene prima sottoposta a SALT e successivamente a HASH utilizzando una funzione HASH crittografica (SHA-512). Ogni account utente ha il proprio valore di SALT univoco. Il Controllo degli accessi è basato sui ruoli (Administrator, Data Manager, Monitor, Osservatore) e l'accesso ai dati è definito in base al ruolo concesso ed in nessun ruolo di default è configurato un accesso globale. Gli owner dei dati del sistema informativo devono condurre annualmente una revisione completa degli account degli utenti. La revisione deve includere quanto segue: • convalidare il ruolo e i diritti correnti dell'utente nel sistema informativo; • revisionare la tabella dei diritti di accesso degli utenti (lettura, scrittura, esecuzione, cancellazione) per garantire "il principio di minimizzazione"; • convalidare che il ruolo dell'utente non è stato combinato con altri ruoli col risultato di attribuzione di privilegi eccessivi. REDCap effettua processi di sanificazione, filtraggio, controllo del tipo di dati ed escape per proteggere dai metodi di attacco,

		come Cross-Site Scripting (XSS) e SQL Injection. Per proteggere in modo specifico dalla Cross-Site Request Forgery (CSRF), che è un altro metodo di attacco, REDCap utilizza un "nonce" (un token segreto specifico dell'utente) su ogni modulo Web utilizzato nell'applicazione. Il nonce viene generato come valore univoco per ogni nuova richiesta HTTP in ogni sessione REDCap. Inoltre, REDCap utilizza la "limitazione della velocità" nelle sue pagine Web, in cui esiste un numero massimo di richieste Web al minuto consentite da un singolo indirizzo IP e, dopo che viene raggiunto tale limite, l'indirizzo IP di quell'utente è permanentemente bannato da REDCap. Il valore limite di frequenza delle richieste al minuto per IP è personalizzabile e può essere modificato all'interno del Centro di controllo di REDCap, se necessario. La limitazione della velocità previene gli attacchi Denial of Service da parte dei bot e previene altri tipi di attacchi degli hacker che richiedono l'invio di molte richieste al server in un breve lasso di tempo, ad esempio con un Breach Attack. Per quanto riguarda in particolare la prevenzione dei Breach Attack, oltre a utilizzare la limitazione della velocità, REDCap emette sempre una stringa invisibile di testo casuale di lunghezza casuale su ogni pagina Web (per nascondere la lunghezza reale della pagina) come tecnica efficace per mitigare tale attacco. L'uso da parte di REDCap di un token univoco su ogni modulo

		web riduce notevolmente anche la possibilità di un Breach Attack. REDCap ha un audit trail integrato che registra automaticamente tutte le attività degli utenti e registra tutte le pagine visualizzate da ogni utente, comprese le informazioni contestuali (ad esempio il progetto o il record a cui si accede). REDCap registra tutte le azioni, indipendentemente dal fatto che l'attività sia l'immissione di dati, l'esportazione di dati, la modifica di un campo, l'esecuzione di un report o l'aggiunta/modifica di un utente. Il record di registrazione può essere visualizzato all'interno di un progetto esclusivamente dagli Amministratori di Sistema su esplicita richiesta dei Contitolari. La pagina Registrazione consente a tali utenti di visualizzare l'intero audit trail per quel progetto e anche di filtrare l'audit trail in vari modi in base al tipo di attività e/o utente. L'audit trail integrato in REDCap consente agli Amministratori di essere in grado di determinare tutte le attività e tutti i dati visualizzati o modificati da un determinato utente. Inoltre, registra: - tutti i login/logout eseguiti con successo e falliti; - aggiunte, cancellazioni e modifiche all'account/privilegi dell'utente; - aggiunte, cancellazioni e modifiche ai parametri di log di sicurezza/controllo; - switch degli Username durante una sessione online; - attività eseguite dagli account con privilegi elevati.

		I dati di produzione (dati personali tutelati da norme e regolamenti) non vengono mai utilizzati nei sistemi di non-produzione a meno che non ci sia una ragione di business per farlo e che i dati siano stati propriamente anonimizzati, mascherati o criptati.
Crittografia	**x**	I Dati Personali sono crittografati sia *at rest* sia *in transit*. In particolare, - i servizi offerti dagli application server di REDCap sono protetti dalla crittografia dei dati trasmessi sulla rete mediante protocollo SSL e certificato digitale a 256 bit emesso da Let's Encrypt (autorità di certificazione open source messa a disposizione dall'organizzazione non-profit Internet Security Research Group -ISRG); - il protocollo di trasporto dei dati verso l'esterno del sistema è crittografato (SSL / TLS / HTTPS); il protocollo di trasporto dei dati tra application server e database è crittografato (SSL / TLS). I Dati Personali salvati nell'eCRF saranno accompagnati dall'ID paziente ("**ID pt.**"), creato secondo quanto di seguito descritto. Lo Sperimentatore principale Fondazione IRCCS (nonché altri soggetti autorizzati in base a quanto stabilito dalle leggi applicabili), ha accesso a un

		documento denominato Name Code File in cui vengono riportati nome, cognome, sesso, data di nascita, data di arruolamento, luogo di residenza, indirizzo e-mail, numero di cellulare, ID pt. Il Name Code File viene conservato sia in formato elettronico sia cartaceo (stampato e sottoscritto) in modo da evitare accessi non autorizzati. La chiave di cifratura del file rimane nella sola disponibilità della Fondazione IRCCS.
Anonimizzazione	**N/A**	
Policy gestione data breach	**x**	Fondazione, qualora venga a conoscenza di una violazione della sicurezza che possa comportare accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai Dati Personali (che sia occorsa anche presso i propri Responsabili del trattamento), si impegna ad adottare le misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente. In particolare: (i) predisporre e aggiornare un registro che dettagli le violazioni dei Dati Personali subite, indicando la natura delle stesse, le categorie d'Interessati coinvolti, le possibili conseguenze e le misure di sicurezza implementate; (ii) valutare se è necessario notificare al Garante l'eventuale violazione della sicurezza e, ove ne ricorrano i presupposti, effettuare la comunicazione agli

		Interessati, nei tempi previsti dall'art. 34.
Misure anti-intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi...)	**x**	L'accesso all'applicativo è riservato agli utenti previa autenticazione, l'autenticazione utilizzata è basata su tabella, che utilizza l'archiviazione di coppie nome utente/password in una tabella del database. Per motivi di sicurezza, la password nella tabella del database non viene archiviata come testo normale, ma viene prima sottoposta a salt e quindi sottoposta a hash utilizzando una funzione hash crittografica SHA-512 prima di essere archiviata nella tabella del database. Ogni account utente ha il proprio valore di salt univoco. Per l'accesso alla Piattaforma è in corso di implementazione l'autentificazione a 2 fattori per qualsiasi tipo di utenza. Per effettuare l'accesso con utenti con privilegi elevati è sempre richiesta l'autentificazione a 2 fattori. Per impedire l'accesso nei casi di allontanamento dalla postazione o nei casi di chiusura della finestra del browser senza aver chiuso la sessione, l'applicativo ha impostato un tempo di disconnessione automatica dopo 15 minuti di inattività ed il tempo massimo di una sessione attiva è di 120 minuti dopo di che sarà richiesto nuovamente l'accesso. Per impedire attacchi di brute force il sistema, dopo 5 tentativi di accesso non riusciti, blocca l'accesso all'utente per 15 minuti. Al fine di proteggere da attacchi dizionario o ibridi è negata all'utente la possibilità di riutilizzo di una password già

		utilizzata (almeno le ultime 5) ed è stata impostata la forzatura del cambio di password ogni 90 giorni.
Gestione politiche di tutela privacy	**x**	La Fondazione ha adottato procedure, istruzioni operative e regolamenti per la protezione dei dati

Tabella dei rischi afferenti alla DPIA

Descrizione del Rischio	**Probabilità**	**Conseguenze**	**Entità complessiva del Rischio**	**Opzioni che permettono di evitare e/o mitigare questo rischio**
PERDITA DI DATI	Poco probabile	Marginali	Basso	Back-up dei dati, controllo degli accessi, misure anti-intrusive, tracciabilità, politiche di sicurezza informatica
MODIFICHE INDESIDERATE	Poco probabile	Marginali	Basso	Istruzione di soggetti autorizzati al trattamento; formazione; procedure rigorose; politiche di tutela privacy; misure anti-intrusive; politiche di sicurezza informatica; controllo accessi (log). Back-up dei dati; antivirus
ACCESSO ILLEGITTIMO	Poco probabile	Marginali	Basso	Formazione adeguata del personale che interagisce con la piattaforma di raccolta dati, misure anti-intrusive, controllo accessi, politiche di sicurezza informatica e di tutela privacy.

Tabella dei rischi afferenti alla DPIA

	PROBABILITA' DELL'EVENTO	**CONSEGUENZE**	**ENTITA' COMPLESSIVA DEL RISCHIO**
1	Improbabile	Trascurabili	Molto Basso
2	Poco probabile	Marginali	Basso
3	Probabile	Limitate	Medio
4	Molto Probabile	Gravi	Alto
5	Quasi Certo	Gravissime	Molto Alto

8. Valutazioni conclusive

Opinione degli interessati o dei loro rappresentanti (ove raccolta)

Parere del Responsabile Protezione Dati (DPO)
Alla luce delle valutazioni effettuate e delle misure tecniche esistenti o pianificate, si ritiene che il rischio per gli interessati sia, nel complesso, marginale e pertanto non si ravvedono problematiche per la conduzione dello studio in oggetto.

Validazione della DPIA

Sottoscrizioni	Firma	Data
Il Responsabile Protezioni dati		
Il Principal Investigator dello Studio	ANGELO VALERIO MARZANO Universita' degli Studi di Milano 14.01.2026 10:01:23 GMT+00:00	

Aggiornamenti successivi:

Data	Aggiornamento