



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

Donazione multiorgano dopo morte cerebrale: variazioni nel corso degli anni

ACRONIMO: DOMUs-MC

Predisposizione: Dott.ssa Federica Ravetti

Valutazione: Avv. Margherita Clerici, Referente privacy per la ricerca

Validazione: Prof.ssa Silvana Castaldi, Data Protection Officer

Stato: Redatta il 18 giugno 2026

Versione: 1.0



Sommario

1. Premessa.....	3
2. Valutazione della necessità di redigere una DPIA	3
3. Definizioni	3
4. Descrizione del trattamento	4
4.1 Finalità del trattamento e contesto dello studio	4
4.2 Responsabilità connesse al trattamento.....	5
4.3 Standard applicabili al trattamento dei dati	6
4.4 Categorie di interessati	6
4.5 Categorie di dati trattati.....	6
4.6 Accesso ai dati.....	7
4.7 Modalità di raccolta e conservazione dei dati: strumento e tecnologie utilizzati	8
5. Principi fondamentali.....	8
5.1 Basi giuridiche che rendono lecito il trattamento dei dati	8
5.2 Periodo di conservazione dei dati	8
6. Misure a tutela degli interessati	8
6.1 Modalità di informazione degli interessati	8
6.2 Modalità di esercizio dei diritti da parte degli interessati	9
7. Rischi	9
7.1 Misure tecniche esistenti o pianificate	9
8. Valutazioni conclusive.....	20



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) è Titolare autonomo 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 **"Donazione multiorgano dopo morte cerebrale: variazioni nel corso degli anni"**.

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: **Donazione multiorgano dopo morte cerebrale: variazioni nel corso degli anni**

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: osservazionale, non farmacologico, retrospettivo, monocentrico, no profit



Lo studio arruolerà pazienti con diagnosi di morte cerebrale, ricoverati presso la Rianimazione ad indirizzo Neurologico, la Terapia Intensiva "VECLA" e la Rianimazione Cardiochirurgica della Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico tra 01/01/1998 al 31/12/2025

Interessati: i soggetti arruolati nello Studio presso la Fondazione a cui i Dati Personali si riferiscono e i Ricercatori e altro personale del Titolare coinvolti nello studio.

Numero dei pazienti previsti per lo studio: 519

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: DOMUs-MC

Promotore: Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico

Centro coordinatore: SC Anestesia e Rianimazione ad Indirizzo Neurologico

Sperimentatore principale: Dott.ssa Chiara Magri

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

Il trapianto di organi solidi è l'unica opzione terapeutica per alcuni pazienti con diverse malattie in stadio terminale. Nonostante il numero di trapianti in Italia sia costantemente aumentato negli anni, il numero di pazienti in lista d'attesa è ancora elevato. Per questo motivo, l'ottimizzazione del procurement di organi rappresenta una priorità in ambito trapiantologico.

I donatori in morte cerebrale (DBD) secondaria a lesioni cerebrali acute costituiscono la maggior parte dei donatori d'organi in Italia. La gestione dei DBD ha come obiettivo il mantenimento della perfusione e della funzionalità dei diversi organi e deve avvenire nei reparti di terapia intensiva. Le alterazioni patofisiologiche conseguenti alla morte cerebrale (perdita di tutte le funzioni cerebrali, alterazioni del tono simpatico, deficit ormonali) richiedono infatti supporti vitali, monitoraggi avanzati e interventi rapidi e mirati. Inoltre, il quadro clinico può essere ulteriormente complicato dalla presenza di patologie croniche o di complicanze sviluppate durante il ricovero in terapia intensiva (infezioni, insufficienza cardiaca, insufficienza respiratoria...).

Nel corso degli ultimi decenni, le caratteristiche epidemiologiche dei pazienti ricoverati in terapia intensiva con lesioni cerebrali acute (trauma cranico, ictus ischemici ed emorragici) si sono modificate parallelamente all'invecchiamento generale della popolazione. Inoltre, i criteri di definizione di rischio e di accettazione utilizzati per determinare l'idoneità di un organo potenzialmente trapiantabile sono stati modificati. Questi due fattori probabilmente hanno determinato una variazione del numero dei potenziali DBD ma anche delle loro caratteristiche. I dati disponibili in letteratura sono però molto limitati.

OBIETTIVI DELLO STUDIO

Obiettivo primario



L'obiettivo primario è calcolare il rapporto tra donatori adulti segnalati (potenziali donatori sottoposti ad accertamento di morte encefalica, segnalati al coordinamento) e donatori adulti utilizzati (donatori dei quali sia stato trapiantato almeno un organo) all'interno della Fondazione (gennaio 1998-dicembre 2025).

Obiettivi secondario dello studio:

1. Valutare la variazione nel tempo del rapporto calcolato per conseguire l'obiettivo primario
2. Valutare i cambiamenti epidemiologici nella tipologia di donatore nell'ipotesi che questi possano influire sia sulla gestione clinica sia sulla tipologia di organi prelevati.
3. Valutare variazioni della gestione clinica del donatore (emodinamica, respiratoria, metabolica, ormonale) e il loro impatto sul numero di organi prelevati e la loro ripresa funzionale post-trapianto

Endpoint

Endpoint primario

Valutare il rapporto tra donatori segnalati e donatori utilizzati nella nostra struttura, espresso in percentuale.

Endpoint secondari

Variazione nel tempo del rapporto tra donatori segnalati e donatori utilizzati nella nostra struttura, espresso in percentuale.

Descrivere le variazioni epidemiologiche del potenziale DBD (età, sesso, patologia d'ammissione, durata del ricovero in terapia intensiva, comorbidità)

Descrivere la variazione nel tempo della gestione clinica (emodinamica, respiratoria, metabolica, ormonale) del potenziale DBD ed identificare una possibile correlazione tra gestione clinica del donatore multiorgano e numero di organi risultati idonei al prelievo. Questo può essere fatto mediante analisi di correlazione tra gestione clinica e outcome dei singoli organi (in termini di donazione effettuata o meno).

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.



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 principi 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

a. Pazienti che presentano le seguenti caratteristiche

Verranno inclusi per questo studio tutti i pazienti che soddisfano i seguenti criteri di inclusione:

- Diagnosi di morte cerebrale secondo la presenza di criteri per l'accertamento di morte cerebrale previsti dalla legislazione italiana (Legge 29 dicembre 1993, n.578, Decreto 22 agosto 1994 n.582 del Ministero della Sanità, Decreto 11 aprile 2008 n. 582) e ricovero presso le strutture della Fondazione tra 01/01/1998 al 31/12/2025.
- Entrambi i sessi
- Età ≥18 anni

b. Personale coinvolto nello studio

4.5 Categorie di dati trattati

Le variabili raccolte includono:

- Età, sesso



- Dati antropometrici
- L'elenco delle comorbidità e dei farmaci assunti prima del ricovero
- Causa di morte encefalica
- Date di ingresso in ospedale e in terapia intensiva, durata della degenza in terapia intensiva ed in ospedale, durata della somministrazione di farmaci, durata della ventilazione meccanica
- Score di gravità utilizzati in terapia intensiva (Glasgow Coma Scale, (GCS), Simplified Acute Physiology Score (SAPS) II, Acute Physiologic Assessment and Chronic Health Evaluation (APACHE) II, Sequential Organ Failure Assessment (SOFA)
- Gli esami ematochimici di routine (emocromo, coagulazione, funzionalità renale ed epatica, indici di flogosi, elettroliti, indici di citolisi)
- Esami colturali eseguiti per normale pratica clinica
- Emogas analisi effettuate sia arteriose che venose
- Parametri respiratori: modalità di ventilazione, ETCO₂, distribuzione regionale della ventilazione mediante EIT
- Parametri emodinamici ottenuti dai monitoraggi invasivi e non invasivi (e.g., mean arterial pressure (PAM), heart rate (HR), stroke volume variation (SVV), intrathoracic total blood volume (ITBI), volume telediastolico globale indicizzato (GED_i), indice cardiaco (CI), indexed systemic vascular resistance (SVRI), central venous saturation (ScVO₂), mixed venous saturation (SVO₂))
- Dati di monitoraggio neurologico (diametro e reattività pupillare, pressione intracranica (ICP) e pressione di perfusione cerebrale (CPP)
- Quantità e tipologia di liquidi somministrati e bilancio idrico giornaliero
- Diuresi giornaliera ed esame urine
- Quantità e tipologia di farmaci somministrati (es: antibiotici, inotropi, vasoattivi...)
- Referti imaging effettuato (ecografie, TAC, RMN)

4.6 Accesso ai dati

Soggetti che accedono ai dati personali

Ad ogni partecipante verrà assegnato un codice univoco. L'identificazione dei dati avverrà in maniera tale 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.

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.

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 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

Al fine di assolvere all'obbligo informativo dei pazienti, ai sensi dell'art. 14 del Regolamento, sarà predisposta e pubblicata sul sito web di Fondazione 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 équipe (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, controllo accessi, 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

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 inserimento 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

Handwritten signature



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 internet 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,
--	--	--

[Handwritten signature]



		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
--	--	---

2



		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.
--	--	--

Handwritten signature



		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 <i>at rest</i> sia <i>in transit</i>. 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

Handwritten signature



		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

24



		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'autenticazione a 2 fattori per qualsiasi tipo di utenza. Per effettuare l'accesso con utenti con privilegi elevati è sempre richiesta l'autenticazione 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



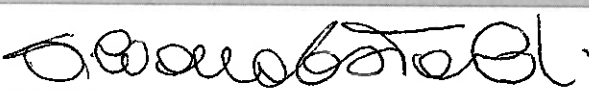
8. Valutazioni conclusive

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		12/03/26

Aggiornamenti successivi:

Data	Aggiornamento