VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

DPIA (Data Protection Impact Assessment)

Trattamento in esame: Ricerca e sperimentazione clinica mediante Piattaforma REDCap

Descrizione del trattamento	Attività di Ricerca e sperimentazione clinica nonché attività amministrative connesse
Titolare del trattamento	Azienda Ospedaliero-Universitaria di Modena
RPD/DPO	dr.ssa Erica Molinari
Data di avvio	aprile 2024
Data validazione DPO	19/07/2024
Frequenza di aggiornamento prevista	Annuale

Contesto generale

Raccolta dati

Nell'ambito della attività di Ricerca, di norma i dati sono forniti direttamente dal soggetto interessato (o da soggetti che esercitano nei confronti dell'interessato la responsabilità genitoriale, o rivestono la qualifica di tutori o amministratori di sostegno) o da soggetti terzi (medico specialista di riferimento, medico di base, ASL, Comune, Autorità diverse, etc.), previa verifica della legittimità del trattamento e della finalità di raccolta anche in coerenza con quanto è definito nel protocollo di Ricerca approvato dal Comitato Etico (CE).

Quando la raccolta dei dati avviene presso i diretti interessati, o persone di riferimento degli stessi, l'informativa e l'acquisizione del consenso, nei casi previsti, sono effettuati nelle forme e con le modalità previste dalle vigenti norme e dalle disposizioni interne in materia.

I dati possono essere acquisiti d'ufficio presso Amministrazioni e gestori di pubblici servizi in relazione ad accertamenti o controlli previsti dalla norma vigente.

I dati possono pervenire alla Azienda anche su comunicazione di soggetti terzi, con riferimento all'accertamento d'ufficio di stati, qualità, e fatti o per il controllo delle dichiarazioni sostitutive presso amministrazioni e gestori di pubblici servizi.

Non verranno inseriti dati personali dell'interessato ma esclusivamente un ID univoco associato all'anagrafica.

L'associazione ID/anagrafica è gestita e archiviata su sistemi informatici differenti ma altrettanto sicuri sotto la responsabilità del PI.

Categorie di dati personali trattati

L'attività di Ricerca prevede il trattamento dei dati personali di soggetti interessati arruolati negli studi condotti presso l'Azienda Ospedaliero-Universitaria di Modena/Titolare del trattamento. Tra questi soggetti rientrano anche pazienti sottoposti a prestazioni sanitarie nell'ambito della normale pratica clinica; i pazienti possono essere anche minori, persone temporaneamente incoscienti (ad es. in coma, e interdetti/inabilitati).

I Dati personali comprendono:

- Dati anagrafici (sesso, data di nascita e luogo di residenza).
- Dati antropometrici, dati relativi alla salute raccolti durante le visite, i ricoveri, gli accessi al pronto soccorso nonché gli esami e gli accertamenti effettuati presso l'Azienda. In particolare, i dati riguardano diagnosi, interventi, terapie somministrate, esiti degli esami di laboratorio, dispositivi, campioni biologici e dati genetici.

Il trattamento di dati per finalità di Ricerca in esame, considerato l'utilizzo di strumenti informatizzati, potrebbe riguardare anche il trattamento dei dati personali dei caregiver e dei rappresentanti dei soggetti in Ricerca, degli operatori convolti nel progetto di Ricerca, tra i quali dati anagrafici, dati di contatto (indirizzo e-mail) e i log delle attività svolte.

L'attività di trattamento oggetto della presente DPIA, dunque, considerate le categorie dei dati personali da trattare potrebbe presentare un rischio elevato per i diritti e le libertà delle persone fisiche, secondo i criteri di cui all'art. 35, paragrafo 3, del GDPR.

La presente DPIA, in particolare, ha ad oggetto il trattamento dei dati personali degli interessati arruolati negli studi condotti con REDCap presso l'Azienda Ospedaliero-Universitaria di Modena/Titolare del trattamento.

Base giuridica

Il GDPR introduce una specifica deroga al divieto di trattamento delle particolari categorie di dati per scopi di Ricerca, ammettendo che essi possano essere trattati per tali scopi sulla base del diritto dell'Unione Europea o nazionale. Tale trattamento dev'essere proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, in conformità dell'articolo 89, paragrafo 1 del Regolamento (art. 9, par. 2, lett. j) del Regolamento).

Nel solco dello spazio normativo definito da tale ultima disposizione, il legislatore italiano ha mantenuto, modificandola – e integrando il GDPR a livello nazionale - la medesima disposizione previgente del Codice Privacy che riguarda la Ricerca medica, biomedica ed epidemiologica, ovvero l'art. 110.

Il comma 1 dell'art. 110, da ultimo modificato dalla L. 56/2024, dispone che *"Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di Ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la Ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la Ricerca rientra in un programma di Ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della Ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di Ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice"*.

La base giuridica, quindi, per finalità di Ricerca e sperimentazione clinica è costituita da:

- art. 9, par. 2 lettera a) del GDPR;
- art. 9, par. 2 lettera j) del GDPR;
- art. 110 del Codice Privacy;
- art. 110-bis del Codice Privacy.

È nel consenso (art. 9, par. 2 lettera a) del GDPR), dunque, che è possibile rinvenire la base giuridica del trattamento di dati per finalità di Ricerca scientifica, seppure siano previste alcune eccezioni.

In effetti, il consenso dell'interessato non è necessario (secondo l'art. 9, par. 2, lettera j) del GDPR e l'art. 110, co. 1 primo periodo del Codice Privacy) quando la Ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione Europea.

Negli altri casi, quando non è possibile acquisire il consenso degli interessati (coerentemente con il Provvedimento dell'Autorità Garante n. 146 del 5 giugno 2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"), è documentata, nel progetto di Ricerca la sussistenza delle ragioni, considerate del tutto particolari o eccezionali, per le quali informare gli interessati risulta impossibile o implica uno sforzo sproporzionato oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della Ricerca, tra le quali in particolare:

1. i motivi etici riconducibili alla circostanza che l'interessato ignora la propria condizione. Rientrano in questa categoria le ricerche per le quali l'informativa sul trattamento dei dati da rendere agli interessati comporterebbe la rivelazione di notizie concernenti la conduzione della Ricerca la cui conoscenza potrebbe arrecare un danno materiale o psicologico agli interessati stessi (possono rientrare in questa ipotesi, ad esempio, gli studi epidemiologici sulla distribuzione di un fattore che predica o possa predire lo sviluppo di uno stato morboso per il quale non esista un trattamento);
2. i motivi di impossibilità organizzativa riconducibili alla circostanza che la mancata considerazione dei dati riferiti al numero stimato di interessati che non è possibile contattare per informarli, rispetto al numero complessivo dei soggetti che si intende coinvolgere nella Ricerca, produrrebbe conseguenze significative per la Ricerca in termini di alterazione dei relativi risultati; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dalla Ricerca, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti (ad esempio, nei casi in cui la Ricerca riguarda interessati con patologie ad elevata incidenza di mortalità o in fase terminale della malattia o in età avanzata e in gravi condizioni di salute). Con riferimento a tali motivi di impossibilità organizzativa, le prescrizioni dell'Autorità concernono anche il trattamento dei dati di coloro i quali, all'esito di ogni ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto presso l'anagrafe degli assistiti o della popolazione residente) risultino essere al momento dell'arruolamento nella Ricerca:
    - deceduti o
    - non contattabili.

    Resta fermo l'obbligo di rendere l'informativa agli interessati inclusi nella Ricerca in tutti i casi in cui, nel corso della Ricerca, ciò sia possibile e, in particolare, laddove questi si rivolgano al centro di

cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento;

3. motivi di salute riconducibili alla gravità dello stato clinico in cui versa l'interessato a causa del quale questi è impossibilitato a comprendere le indicazioni rese nell'informativa e a prestare validamente il consenso. In tali casi, la Ricerca deve essere volta al miglioramento dello stesso stato clinico in cui versa l'interessato. Inoltre, occorre comprovare che le finalità della Ricerca non possano essere conseguite mediante il trattamento di dati riferiti a persone in grado di comprendere le indicazioni rese nell'informativa e di prestare validamente il consenso o con altre metodologie di Ricerca. Ciò, avuto riguardo, in particolare, ai criteri di inclusione previsti dalla Ricerca, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché all'attendibilità dei risultati conseguibili in relazione alle specifiche finalità della Ricerca. Con riferimento a tali motivi, deve essere acquisito il consenso delle persone indicate nell´art. 82, comma 2, lett. a), del Codice come modificato dal d.lgs. n. 101/2018. Ciò, fermo restando che sia resa all'interessato l'informativa sul trattamento dei dati non appena le condizioni di salute glielo consentano, anche al fine dell'esercizio dei diritti previsti dal Regolamento.

In coerenza con le più recenti pronunce dell'Autorità Garante, l'impossibilità di acquisire il consenso è accertata in occorrenza di tre tentativi infruttuosi di raccolta.

Infine, tra gli altri, si richiamano i seguenti riferimenti:

1. Dichiarazione di Helsinki (WMA Declaration Of Helsinki – Ethical Principles For Medical Research Involving Human Subjects).

2. Convenzione di Oviedo "per la protezione dei Diritti dell'Uomo e della dignità dell'essere umano nei confronti dell'applicazione della biologia e della medicina: Convenzione sui Diritti dell'Uomo e la biomedicina" del 4 aprile 1997.

3. Clinical Trials Regulation (Regulation (EU) No 536/2014).

4. Regole Deontologiche per trattamenti a fini statistici o di Ricerca scientifica (Provvedimento dell'Autorità Garante del 19 dicembre 2018 n. 515), modificato con Provvedimento n. 298 del 9 maggio 2024, al fine di individuare le garanzie di cui all'art. 110, comma 1, del Codice Privacy, a seguito della modifica intervenuta con la L. 56/2024.

5. Provvedimento dell'Autorità Garante n. 146 del 5 giugno 2019 recante le "Prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"

6. Regolamento Regione Emilia-Romagna (RER) n. 1/2014 Allegato B.

Informativa e Consenso

Il trattamento dei dati personali, effettuato nell'ambito della Ricerca, nelle sue diverse forme è descritto in forma chiara ed intellegibile, nell'informativa ex artt. 13 e 14 del GDPR, in cui sono elencate finalità e modalità del trattamento quale condizione principale del dovere del titolare di assicurare la trasparenza e la correttezza dei trattamenti effettuati.
L'informativa resa ai sensi dell'art. 13 del GDPR (o dell'art. 14 GDPR nel caso in cui i dati non siano stati ottenuti presso l'interessato) viene fornita all'interessato (ivi compresi genitori/tutori/amministratori di sostegno) arruolabile nella Ricerca, di norma durante l'incontro di presentazione della Ricerca o, nel caso degli studi retrospettivi, durante un contatto successivo alla raccolta del dato.
In tale occasione, ove necessario e possibile, viene anche raccolto il consenso specifico al trattamento dei dati.

Nell'informativa sono, altresì, comunicati agli interessati la durata della Ricerca e i tempi di trattamento e conservazione dei dati.

Pubblicazione

Ai sensi dell'art. 110, comma 1, secondo periodo del Codice Privacy e nel rispetto delle garanzie individuate dal Provvedimento dell'Autorità Garante n. 298 del 9 maggio 2024, nel caso di studi che prevedano trattamenti di dati sulla salute per finalità di ricerca medica, biomedica e epidemiologica, riferiti a soggetti deceduti o non contattabili per motivi etici o organizzativi, la Valutazione d'impatto è oggetto di pubblicazione sul sito web istituzionale della Azienda, nella sezione dedicata all'attività di Ricerca.

Unitamente alla DPIA sarà resa pubblica anche l'informativa per il trattamento dei dati personali, resa ai sensi dell'art. 13 del GDPR (o dell'art. 14 GDPR nel caso in cui i dati non siano stati ottenuti presso l'interessato).

Attività di Ricerca condotta sulla piattaforma REDCap

Premessa

La piattaforma REDCap (Research Electronic Data Capture), costituita nel 2004 dalla Vanderbilt University, permette di creare, in modo gratuito e sicuro, schede di raccolta dati elettroniche a supporto di varie fasi di un progetto di Ricerca: creare la scheda di raccolta dati (eCRF), monitorare la qualità del dato inserito (ad es. formato, range, coerenza con campi complementari), creare report automatici per il monitoraggio della Ricerca, esportare i dati raccolti in formati adatti a successive elaborazioni statistiche.

L'impiego di REDCap, per le esigenze dell'attività di Ricerca riguarderà tutte le strutture della Azienda, ad eccezione dei casi nei quali i partecipanti alla Ricerca decidano di servirsi di altro applicativo.

Il software è disponibile gratuitamente per i partner del consorzio REDCap, consente di gestire progetti mono o multi-sito ed è completamente personalizzabile e configurabile. Il fornitore della piattaforma REDCap non accede ad alcun dato personale inserito dalla Azienda Ospedaliero-Universitaria di Modena e non necessita di nomina a Responsabile del trattamento a norma dell'art. 28 GDPR.

Elementi caratteristici di REDCap

La piattaforma REDCap permette di:

- progettare, costruire e mettere in opera database per raccolta dati di studi mono o multicentrici,
- di raccogliere dati su un server privato, accessibile esclusivamente tramite account personale,
- gestire la qualità del dato configurando il sistema in modo tale che vi siano dei controlli sui dati inseriti (formato, range ecc.),
- creare query automatiche e manuali per il monitoraggio della Ricerca,
- esportare i dati raccolti nei formati utili per le elaborazioni statistiche.

Criteri e Metodologia

Valutazione preliminare dell'utilizzo dei dati

Come verranno raccolti i dati?

L'attività di Ricerca e di sperimentazione clinica, analizzata dal presente documento, prende in esame i dati personali, compresi i dati di natura particolare, raccolti attraverso varie fonti a seconda della tipologia della Ricerca da realizzare. Di seguito si elencano sinteticamente, a titolo di esempio, alcune fonti di raccolta dei dati:

a) interessati;
b) cartelle cliniche ed ambulatoriali;
c) database e applicativi;
d) open data;
e) dataset prodotti da soggetti pubblici o privati, nazionali o internazionali;
f) database interni ed esterni;
g) biobanche;
h) applicativi informatici;
i) dispositivi elettronici;
j) IOT (Internet of Things);
k) data lake.

Chi avrà accesso ai dati?

Per le attività di Ricerca e di sperimentazione clinica: PI e soggetti dell'equipe di Ricerca

Per le attività di rimborso delle spese sostenute dai soggetti arruolati nella Ricerca: l'Ufficio competente individuato dall'Azienda/Istituto.

Tutti i soggetti sopra elencati sono delegati o autorizzati al trattamento dei dati nel rispetto della policy aziendale.

Accesso ai dati in REDCap

L'accesso ai dati contenuti nella piattaforma REDCap è consentito ai soggetti autorizzati al trattamento ed avviene tramite profilatura e autenticazione strettamente legata alle funzioni svolte.

Il sistema è predisposto per sfruttare diverse tipologie di autenticazione con modalità singola o a doppio fattore nel caso in cui i dati siano esposti su internet.

La gestione delle utenze e degli studi, che avviene attraverso cruscotti ben definiti ad opera del PI o da un suo delegato, permette di stabilire una serie di parametri tra cui: la durata di validità, complessità della password e intervallo di rinnovo della stessa. Le utenze, inoltre, sono agganciate allo specifico progetto e ogni singolo profilo può essere abilitato ad avere accesso a più studi.

L'abilitazione all'accesso dei dati dopo la cessazione della Ricerca è definita in funzione del ruolo svolto nella Ricerca dall'amministratore di sistema.

Per i centri esterni la validità delle utenze sarà comunque limitata al periodo della sperimentazione.

L'accesso può essere consentito ad altre strutture, pubbliche o private, a seconda della tipologia di progetto/Ricerca.

In che modo i dati verranno eventualmente trasferiti/comunicati a soggetti terzi?

Il trasferimento di documenti contenenti dati raccolti all'interno degli Studi può avvenire attraverso:

- la PEC;

- la posta elettronica ordinaria, in tal caso allegando i documenti de quo in formato criptato e inviando la chiave di decriptazione con altro strumento di comunicazione;
- altri strumenti di sicurezza in uso presso l'Azienda Ospedaliero-Universitaria di Modena (es. cloud).

Attraverso i processi di autenticazione e autorizzazione, i destinatari dei dati potranno accedere alle piattaforme condivise per l'estrazione del dataset.

La comunicazione e il trasferimento dei dati per i trattamenti connessi alla presente valutazione d'impatto può avvenire previa sottoscrizione di un accordo specifico e comunque, in coerenza con quanto previsto dalla normativa vigente e pattuito nel protocollo di Ricerca.

Come verranno archiviati, aggiornati ed eliminati i dati quando non più necessari?

I dati relativi agli studi saranno aggiornati in funzione delle attività svolte nelle varie fasi previste della Ricerca stessa, archiviati per il tempo definito in ogni protocollo di Ricerca ed eliminati al termine temporale anch'esso definito nel protocollo di Ricerca e nell'informativa per il trattamento dati personali.

I dati contenuti nelle fonti, di cui sopra, seguono il ciclo di vita proprio definito dalla normativa di settore (massimario di scarto).

Valutazione del rischio

Metodi di identificazione degli interessati

In ossequio alle procedure e ai regolamenti Aziendali, il riconoscimento dei soggetti reclutati avviene attraverso sistemi tradizionali, quali ad esempio la carta di identità o altro documento di riconoscimento. Negli studi retrospettivi l'identificazione può essere effettuata anche attraverso codificazioni derivanti da numeri nosologici o codici di pseudonimizzazione assegnati in fase di rilevazione e registrati in appositi Database.

Allo stato attuale non sono previsti ulteriori metodi di identificazione intrusivi e/o onerosi per l'interessato (es. dati biometrici).

Coinvolgimento di altre strutture

Nelle ricerche che coinvolgono più di un centro partecipante/collaborante (ad es. negli studi multicentrici) il coinvolgimento di altri soggetti pubblici o privati viene regolato da atti giuridici che definiscono compiti e responsabilità.

L'attività di Ricerca di tipo multicentrico prevede la partecipazione di soggetti pubblici o privati (anche appartenenti a enti no profit e di volontariato) nelle modalità previste dal protocollo di Ricerca.

Modifiche alle modalità di trattamento dei dati

Il trattamento mediante la piattaforma REDCap non apporterà nuove o significative modifiche alle modalità di trattamento dei dati personali tali da destare preoccupazioni dell'interessato. Inoltre, l'informativa resa agli interessati contiene tutti gli elementi necessari a far sì che il trattamento sia compreso in tutte le sue fasi e modalità di esecuzione.

I dati personali, propri di un interessato, già presenti in un esistente database, non verranno assoggettati a nuove o modificate modalità di trattamento, in quanto nei casi in cui la Ricerca sia retrospettiva la fonte dei dati è costituita dai documenti clinici formati per finalità di cura, quindi non modificabili, diversamente da quanto accade negli studi prospettici dove i dati vengono trattati su CRF predisposte ad hoc, sempre tenendo conto dei principi generali che regolano il corretto trattamento dei dati personali.

Per quanto riguarda eventuali nuove o significative modifiche alle modalità di consolidamento, interscambio, riferimenti incrociati, abbinamento di dati personali, provenienti da più sistemi di trattamento che dovessero verificarsi mediante l'utilizzo della piattaforma REDCap, si specifica che tale utilizzo potrebbe modificare le modalità di trattamento in uso, tuttavia ciò avverrà a seguito dell'adozione di misure di sicurezza adeguate, così come previsto dall'art. 32 del GDPR e descritto nell'informativa ex art. 13 e 14 GDPR.

Modifiche alle procedure di trattamento dei dati

Si ritiene che il trattamento mediante la piattaforma REDCap sia sufficientemente trasparente e che non si possano verificare situazioni di intrusività nella sfera personale non conosciuta o non condivisa. L'informativa resa agli interessati contiene tutti gli elementi che descrivono le modalità di raccolta.

Le modalità di conservazione non verranno innovate o modificate. I riferimenti riguardo ai tempi di conservazione sono espressamente indicati e resi conosciuti attraverso l'informativa e fanno riferimento al protocollo di Ricerca o sono determinati dal massimario di scarto.

Il trattamento non prevede una modifica alle modalità con le quali i dati sono messi a disposizione.

Esenzioni dalla applicazione delle disposizioni del GDPR (ex art.2, comma 2 GDPR)

Il trasferimento dei dati personali verso Paesi al di fuori dello Spazio Economico Europeo (extra UE) i dati avverrà esclusivamente nel caso in cui sia stata emanata una decisione di adeguatezza, allo stato attuale Andorra, Argentina, Australia (Passenger Name Record), Canada, Isole FaerOer, Giappone, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA o nei seguenti casi:

- se l'interessato è stato informato dal titolare dell'assenza di una decisione di adeguatezza e dei conseguenti rischi e ha espresso il proprio consenso al trasferimento;
- sulla base di accordi/contrattuali stipulati che forniscono garanzie adeguate agli interessati (CCs Clausole Contrattuali Standard);
- per i gruppi di imprese, (così come disciplinati dal GDPR e secondo la classificazione del Codice Civile, ad es. imprese collegate/partecipate) il trasferimento deve avvenire sulla base di norme vincolanti di impresa che devono essere approvate dall'autorità competente (in Italia, l'Autorità Garante della Privacy);
- il trasferimento è necessario per l'esecuzione di un contratto concluso su richiesta dell'interessato e il titolare;
- sulla base dell'adesione al Data Privacy Framework (DPF), che consente una tutela adeguata degli interessati nei trasferimenti di dati personali tra Europa e Stati Uniti d'America.

Identificazione preliminare dei rischi

L'assessment effettuato ha preso in considerazione i seguenti rischi:

- Distruzione
- Perdita

- Distribuzione non autorizzata
- Accesso ai dati non autorizzato
- Trattamento non autorizzato
- Trattamento non conforme alla finalità della raccolta o illecito

Per ognuno di essi è stata fatta una attenta e approfondita disamina, anche in rapporto alle peculiarità proprie degli studi e sono state adottate le misure di sicurezza adeguate a mitigare i potenziali rischi per i diritti e le libertà degli interessati.

I dati raccolti su eCRF di REDCap, in ossequio al principio di minimizzazione, sono esclusivamente quelli definiti nel protocollo della Ricerca e sono resi in forma pseudonimizzata ed inseriti nella piattaforma REDCap o in altre piattaforme messe a disposizione dai Partner di progetto.

La tabella seguente illustra i principali rischi afferenti al trattamento dei dati e che sono stati identificati in fase di valutazione preliminare.

	Descrizione del rischio	**Valutazione preliminare di esposizione**
Rischio 1	Distruzione	Basso
Rischio 2	Perdita	Basso
Rischio 3	Distribuzione non autorizzata	Medio
Rischio 4	Accesso ai dati non autorizzato	Medio
Rischio 5	Trattamento non autorizzato	Medio
Rischio 6	Trattamento non conforme alla finalità della raccolta o illecito	Medio

Decisione su come procedere

Tenendo conto della tipologia di trattamento e in conformità delle indicazioni previste all'articolo 35, paragrafo 3 del Regolamento Generale sulla protezione dei dati – Regolamento (UE) 2016/679 – GDPR, è necessario effettuare la DPIA sul trattamento della Ricerca in ogni sua declinazione.

Congruità con altre leggi, codici o regolamenti afferenti alla protezione dei dati

In relazione al provvedimento dell'Autorità Garante n. 146/2019, è stata effettuata una verifica di conformità al medesimo, come parte di questa DPIA, secondo quanto illustrato nell'Appendice A e si è giunti alla conclusione che l'attività di trattamento oggetto della presente DPIA è conforme alle prescrizioni del provvedimento indicato.

Descrizione analitica delle operazioni di trattamento, con indicazione delle finalità perseguite dal Titolare del Trattamento

I dati personali degli interessati, compresi quelli appartenenti a particolari categorie e i dati soggetti a maggior tutela (quali quelli dei soggetti minori, donne vittime di violenza, ecc..) sono raccolti e trattati per finalità di Ricerca le cui caratteristiche e modalità sono descritte nel dettaglio nell'informativa ex art. 13 GDPR e nel protocollo della Ricerca.

Valutazione della necessità e proporzionalità delle operazioni di trattamento, in relazione alle finalità

La necessità e la proporzionalità delle operazioni di trattamento si valutano in maniera positiva in quanto sono presenti le seguenti misure:

- finalità determinate, esplicite e legittime;
- liceità del trattamento;
- dati personali adeguati, pertinenti e limitati a quanto necessario;
- limitazione della conservazione.

Valutazione dei rischi che incidono sui diritti e le libertà degli interessati, incluso il rischio di discriminazione connesso o rinforzato dal trattamento

L'analisi condotta, nelle sezioni precedenti, tenendo conto delle misure tecniche ed organizzative nonché degli atti giuridici che talora sottendono il trattamento e che ne disciplinano le forme e le responsabilità degli attori (ad es. accordo di contitolarità, designazione responsabile di trattamento, accordi studi specifici), non ha rilevato rischi che possano incidere sui diritti e le libertà degli interessati.

Descrizione delle misure individuate per mettere sotto controllo i rischi e ridurre al minimo il volume di dati personali da trattare - Data Protection by Default

Al fine di ridurre il rischio per i diritti e le libertà fondamentali degli interessati è prevista la piena applicazione dei principi affermati dall'art. 5 GDPR. Nel dettaglio, i principi di:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Dette misure prevedono disposizioni in materia di sicurezza fisica e logica dei sistemi elencate all'Appendice C

Elenco dettagliato delle salvaguardie, delle misure di sicurezza e dei meccanismi adottati per garantire la protezione dati personali, al fine di dimostrare la congruità con il Regolamento, tenendo conto dei diritti e dei legittimi interessi degli interessati ed altre persone coinvolte

In relazione alle misure di sicurezza infrastrutturali ed organizzative di seguito si elencano le seguenti:

Pseudonimizzazione

A ciascun soggetto arruolato nella Ricerca viene assegnato un ID alfa-numerico/numerico. La corrispondenza tra tale ID e l'identificativo univoco del paziente è conservata all'interno di uno schema separato. Tale schema è gestito nel Delegation Log della Ricerca da personale individuato e autorizzato dal Titolare.

Crittografia delle password

Le password degli utenti vengono memorizzate in formato criptato, ovvero utilizzando algoritmi e altre tecniche per avere un'elevata resistenza agli attacchi.

Crittografia dei dati in transito

Qualora si renda necessario procedere alla comunicazione o trasferimento dei dati, essi vengono crittografati durante la trasmissione tra le diverse componenti del sistema, anche quando i dati vengono inviati da una applicazione web a un server. L'utilizzo di protocolli di crittografia come HTTPS (TLS > 1.2) per le comunicazioni web è essenziale per proteggere i dati durante il transito.

Controllo degli accessi logici

La sicurezza degli accessi nella componente server è assicurata attraverso privilegi di accesso relativi alle singole funzioni erogabili dal sistema rispetto ad ogni dataset in esso contenuto, ovvero vengono collegati a specifici ruoli coerentemente con il Delegation Log. Inoltre, l'autenticazione può essere gestita utilizzando l'interfaccia LDAP oppure può essere configurata con una two-factor authentication.

Tracciabilità

La tracciabilità dei dati viene garantita attraverso diversi meccanismi:

- L'utilizzo di log per registrare le operazioni effettuate sul database da parte degli utenti o dei processi autorizzati.
- L'utilizzo di tabelle di log per registrare la data e l'ora di creazione, modifica o cancellazione dei record del database.
- L'utilizzo di controlli di qualità per valutare la completezza, l'accuratezza, la consistenza e la validità dei dati.

Archiviazione

I tempi di archiviazione dei dati sono, di norma, definiti nel protocollo di Ricerca o dal massimario di scarto.

Controllo degli accessi fisici

L'accesso fisico ai locali che ospitano i server viene regolato dal responsabile STI aziendale, attraverso misure che possono prevedere a seconda dei casi: accesso con badge, area video sorvegliata, ecc.

La tenuta di eventuali dati su supporto cartaceo avviene in armadi chiusi a chiave, con accesso limitato al solo personale autorizzato.

Minimizzazione dei dati

In ossequio al principio di minimizzazione vengono trattati esclusivamente i dati indicati nel dataset necessari per le finalità, degli obiettivi della Ricerca, attraverso la CRF e/o eCRF.

L’accesso all’identificativo univoco del paziente è permesso solo ove strettamente necessario ad un numero limitato di soggetti, coerentemente con il Delegation Log.

Vulnerabilità

Viene assicurata la protezione relativamente alle vulnerabilità software attraverso l’attuazione di una manutenzione ordinaria per l’applicazione di eventuali patch di sicurezza.

Inoltre, la protezione relativamente alle possibili vulnerabilità software è garantita attraverso una costante attività di

- formazione del personale incaricato al trattamento dei dati;
- sviluppo sicuro di procedure di pseudonimizzazione;
- aggiornamento del sistema almeno annuale;
- piani di risposta agli incidenti.

Lotta contro il malware

La misura più importante è tesa ad evitare l’accesso indiscriminato. Inoltre, è previsto il controllo periodico della sicurezza dei server verificando che:

- l'antivirus sia presente, aggiornato e funzionante e che non risultino problemi dalle ultime scansioni;
- non vi sia evidenza di traffico di rete anomalo in uscita, dalla data di ultima verifica

Backup

Il Titolare è responsabile delle procedure di backup a livello di virtualizzazione o, copia periodica del server. Sono impostati backup giornalieri e retention di almeno 30 giorni su server separati

Manutenzione

La manutenzione del server fisico è demandata al personale dello STI aziendale.

Sicurezza dei canali informatici

Il Firewall è adeguatamente configurato dal personale dello STI aziendale.

Sicurezza dell'hardware

Le configurazioni di sicurezza relative all’hardware sono demandate al personale dello STI aziendale.

Protezione contro fonti di rischio non umane

La presenza di backup giornalieri e retention di almeno 30 giorni su server separati evita la perdita di dati.

Inoltre vengono effettuati periodicamente controlli per evitare guasti, difetti dell’architettura IT, alimentazione, rischi ambientali.

Misure organizzative

In relazione alle misure di sicurezza infrastrutturali ed organizzative di seguito si elencano le seguenti:

- Gestione postazioni e dei dispositivi Aziendali
- Designazione del delegato e degli autorizzati al trattamento e indicazione delle istruzioni
- Policy in materia di protezione dei dati
- Policy per la gestione degli incidenti di sicurezza e le violazioni dei dati personali
- Gestione del personale
- Gestione dei terzi che accedono ai dati
- Vigilanza sul rispetto della prescrizione della normativa sulla protezione dei dati

Illustrazione di quali procedure di data protection by design e data protection by default verranno adottate, in conformità all'articolo 32 GDPR

Gli interessati vengono informati nello specifico delle finalità e delle modalità di raccolta dati e verrà acquisito e conservato, ove previsto e possibile, il loro esplicito consenso al trattamento.

Verranno raccolte solo le informazioni necessarie ai fini della Ricerca e di norma vengono seguite le procedure per pseudonimizzare i dati. I dati raccolti all'interno della Ricerca sono registrati su CRF e/o eCRF e gestiti nella piattaforma RDECap, con accesso limitato al PI e ai suoi delegati tramite credenziali personali.

Revisione ed aggiornamento, con riesame di congruità con le esigenze di protezione dei dati - art 35 GDPR

Il riesame di congruità del presente documento sarà effettuato di norma con cadenza annuale; tale periodo può variare in rapporto alle eventuali criticità rilevate durante le fasi del trattamento o a seguito di interventi normativi, regolatori, audit, eventuali modifiche organizzative che possono determinarsi nel corso della Ricerca.

In tal caso, la revisione della DPIA verrà effettuata tempestivamente.

Conclusione

Il percorso si è concluso con la redazione di un documento articolato e completo che, come previsto dall'art. 35 del GDPR, è stato sottoposto a valutazione del DPO.

Il DPO dopo aver valutato che il trattamento si colloca in una gradazione di rischio *Basso,* come da analisi sintetizzata nell'Appendice B, quindi tale da non attivare il procedimento di consultazione preventiva all'Autorità Garante, ha espresso parere favorevole all'utilizzo della piattaforma REDCap presso l'Azienda Ospedaliero-Universitaria di Modena/titolare del trattamento, con la raccomandazione di effettuare il riesame del documento almeno annualmente.

APPENDICE A - Lista di controllo della congruità del trattamento previsto con le esigenze di protezione dei dati

Domanda	Risposta
1. Quali categorie di dati personali vengono trattate?	Dati personali (età, sesso ecc.), dati clinici (diagnosi, trattamenti sanitari, trattamenti farmacologici, esiti di esami di laboratorio, esiti di visite cliniche specialistiche, dati genetici, ecc.)
2. Se vengono trattati speciali categorie di dati, elencati all'articolo 9 comma 1 GDPR, sulla base di quanto illustrato nella DPIA, esiste una motivazione legittima per il trattamento?	Sì, quale parte fondamentale del processo di conduzione dell'attività di Ricerca.
3. Vi sono aspetti afferenti al rispetto dell'articolo 2, comma 2, del GDPR, che protegge i diritti fondamentali e le libertà delle persone fisiche, ed in particolare il loro diritto alla protezione dei dati personali, che non siano trattati in questa DPIA?	NO
4. Tutti i dati personali che verranno trattati sono coperti da garanzie di riservatezza? Se sì, come viene garantita?	I dati vengono trattati solo da soggetti autorizzati inoltre ogni caso i dati sono pseudonimizzati o anonimizzati.
5. Come viene offerta agli interessati l'informativa in merito al fatto che i loro dati personali verranno raccolti e trattati?	L'informativa ai sensi dell'art. 13 o 14 GDPR viene fornita all'interessato, reclutato nella Ricerca, di norma durante l'incontro di presentazione della Ricerca o, nel caso degli studi retrospettivi, possibilmente durante un contatto successivo alla raccolta del dato. In tale occasione, ove necessario e possibile, viene anche raccolto il consenso specifico al trattamento dei dati. L'informativa viene inoltre pubblicata sul sito istituzionale dell'Azienda.
6. Il trattamento dei dati comporta l'utilizzo di dati personali già raccolti, che verranno utilizzati per finalità secondarie?	La possibilità del riuso deve essere descritta nell'informativa degli studi da cui provengono i dati e occorre aver acquisito, ove necessario e possibile, un nuovo consenso specifico.
7. Quali procedure vengono adottate per verificare che le modalità di raccolta dei dati sono adeguate, coerenti e non eccessive, in relazione alle finalità per i quali i dati vengono trattati?	Al fine di ridurre il rischio per i diritti e le libertà fondamentali degli interessati è prevista la piena applicazione dei principi affermati dall'art. 5 GDPR.
8. Con quali modalità viene verificata la accuratezza	L'accuratezza dei dati personali raccolti viene

dei dati personali raccolti e trattati?	garantita mediante gli identificatori utilizzati per l'estrazione: nome, cognome, data di nascita e codice fiscale dei pazienti inclusi nella Ricerca.
9. È stata effettuata una valutazione circa il fatto che il trattamento dei dati personali raccolti potrebbe causare danni ai diritti e alle libertà agli interessati coinvolti?	Sì, tuttavia, non si ritiene che il trattamento effettuato, nelle varie fasi di Ricerca, possa causare danni ai diritti e alle libertà degli interessati coinvolti in ragione delle misure di sicurezza adottate.
10. È stato stabilito un periodo massimo di conservazione dei dati?	I dati saranno conservati fino al termine della Ricerca, salvo che gli interessati acconsentano alla conservazione per un periodo più lungo nell'ambito delle finalità del trattamento. Allo scadere del termine definito nel protocollo di Ricerca i dati verranno distrutti o resi anonimi provvedendo alla cancellazione definitiva e irreversibile della corrispondenza tra il codice utilizzato sul dato e l'associazione di tale codice all'identità del partecipante.
11. Quali misure tecniche e organizzative di sicurezza sono state adottate per prevenire qualsivoglia trattamento di dati personali non autorizzato o illegittimo?	Accesso ai dati riservato – Solo personale avente diritto nell'ambito delle funzioni a cui è normalmente preposto accederà ai dati al fine di estrazione o immissione. Ognuna delle persone coinvolte nell'estrazione o immissione dei dati avrà accesso esclusivamente al sistema o ai documenti a cui è normalmente preposto. Pseudonimizzazione - il dataset in input, a seguito del processo di pseudonimizzazione restituirà in output il dataset pseudonimizzato, modificato rispetto al dato originale, e il dataset di transcodifica depositato su repository Aziendale ad accesso riservato mediante password. Gestione postazioni: le postazioni utilizzate sono principalmente in dominio aziendale e le misure adottate sono quelle previste da regolamenti e policy Aziendali. Controllo degli accessi fisici: l'accesso ai locali è consentito al solo personale che abbia necessità di accedere a dispositivi o attrezzature necessarie al trattamento, conservate in tali locali. Sicurezza dei documenti cartacei: in base alle istruzioni generali impartite dal Titolare, ogni singolo soggetto coinvolto nel trattamento dati

	per finalità di Ricerca, condivide la documentazione prodotta con i soli appartenenti all'equipe di Ricerca. Normalmente la documentazione cartacea riguarda i dati del progetto (es. Protocollo, parere CE) poiché i dati personali relativi ai soggetti coinvolti vengono trattati in modalità informatizzata. Sicurezza dei canali informatici: tutte le postazioni e i dispositivi aziendali sono equipaggiati con strumenti di antispam, antivirus, sistemi di monitoraggio degli apparati fisici di rete e server e gestione degli alert. Gestione delle politiche di tutela della privacy: Il Titolare ha adottato Privacy Policy Aziendali periodicamente revisionate, condivise con tutto il personale. Il personale viene adeguatamente formato in merito alle attività di trattamento e alle misure di sicurezza da adottare.
12. È previsto il trasferimento di dati personali in un Paese non facente parte dell'Unione europea? Se sì, quali provvedimenti sono stati adottati per garantire che i dati siano salvaguardati in modo appropriato?	Per i Paesi al di fuori dello Spazio Economico Europeo (extra UE) i dati saranno trasferiti esclusivamente nel caso in cui sia stata emanata una decisione di adeguatezza, allo stato attuale Andorra, Argentina, Australia (Passenger Name Record), Canada, Isole FaerOer, Giappone, Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA o nei seguenti casi: - se l'interessato è stato informato dal titolare dell'assenza di una decisione di adeguatezza e dei conseguenti rischi e ha espresso il proprio consenso al trasferimento; - sulla base di accordi/contratti stipulati che forniscono garanzie adeguate agli interessati (CCS - Clausole Contrattuali Standard); - per i gruppi di imprese (così come definiti al paragrafo 8.6.1), il trasferimento deve avvenire sulla base di norme vincolanti di impresa che devono essere approvate dall'autorità competente (in Italia, il Garante della Privacy); - il trasferimento è necessario per l'esecu-

	zione di un contratto concluso su richiesta dell'interessato e il titolare; – sulla base dell'adesione al DPF (Data Privacy Framework che consente una tutela adeguata degli interessati nei trasferimenti di dati personali tra Europa e Stati Uniti d'America).

APPENDICE B - Tabella dei rischi afferenti alla DPIA

Descrizione del rischio	Rischi inerenti alla protezione dei dati			Opzioni che permettono di evitare o mitigare questo rischio (opzioni/controlli applicati)	Rischi residui		
	Impatto	Probabilità	Rischio		Impatto	Probabilità	Rischio
Distruzione	1	2	BASSO	Backup, monitoraggio, formazione	1	2	BASSO
Perdita	2	2	BASSO	Backup, monitoraggio, formazione	2	2	BASSO
Distribuzione non autorizzata	2	3	MEDIO	Formazione, stratificazione delle autorizzazioni	1	2	BASSO
Accesso ai dati non autorizzato	2	4	MEDIO	Accesso ai dati riservato. Pseudonimizzazione. Gestione postazioni. Controllo degli accessi fisici. Sicurezza dei documenti cartacei. Sicurezza dei canali informatici. Gestione delle politiche di tutela della privacy. Formazione. Stratificazione delle autorizzazioni, PW rinforzata per accedere ai dati (di norma doppia PW), limitazione dei soggetti che hanno accesso ai dati,	2	2	BASSO
Trattamento non autorizzato	2	3	MEDIO	Accesso ai dati riservato. Pseudonimizzazione. Gestione postazioni. Controllo degli accessi fisici. Sicurezza dei documenti cartacei. Sicurezza dei canali informatici. Formazione. Stratificazione delle autorizzazioni,	1	2	BASSO
Trattamento non conforme alla finalità della raccolta	2	2	BASSO	Accesso ai dati riservato. Pseudonimizzazione. Gestione postazioni.	2	2	BASSO

o illecito				Controllo degli accessi fisici. Sicurezza dei documenti cartacei. Sicurezza dei canali informatici. Formazione. stratificazione delle autorizzazioni,			

LEGENDA

Probabilità (P)		
1	molto bassa	accade solo in circostanze eccezionali (P < 5%)
2	bassa	è improbabile che accada (5% < P < 20%)
3	media	può accadere in un certo numero di casi (20% < P < 50%)
4	alta	avviene in una buona parte dei casi (50% < P < 75%)
5	molto alta	avviene nella maggior parte dei casi (P > 75%)

	Probabilità (P)				
Impatto (I)	molto bassa (1)	bassa (2)	media (3)	alta (4)	molto alta (5)
molto bassa (1)	1	2	3	4	5
bassa (2)	2	4	6	8	10
media (3)	3	6	9	12	15
alta (4)	4	8	12	16	20

molto alta (5)	5	10	15	20	25

Area	Livelli	Entità di rischio
B	1-4 (rischio accettabile)	bassa (B)
M	5-14 (rischio da ridurre)	media (M)
A	15-25 (rischio da ridurre immediatamente)	alta (A)

Per il Titolare
Il Direttore Generale
Dr. Claudio Vagnini
(firmato digitalmente)