VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI AI SENSI DELL'ART. 35 DEL GDPR
PER LO STUDIO DAL TITOLO "*LA ASIMMETRIA DELLE LESIONI ENDOMETRIOSICHE COME DIMOSTRAZIONE DELLA TEORIA DEL REFLUSSO MESTRUALE E DELLE NICCHIE ANATOMICHE: STUDIO MULTICENTRICO ITALIANO DEL GRUPPO ETIC*"

SOMMARIO:

1. PREMESSE……pag.3
2. VALUTAZIONE NECESSITA' DPIA……pag.3
3. DEFINIZIONI……pag.4
4. DESCRIZIONE DEL TRATTAMENTO……pag. 5
   4.1 Finalità del trattamento ……pag.5
   4.2 Responsabilità connesse al trattamento……pag 6
   4.3 Standard Applicabili al trattamento dei dati……pag 6
   4.4 Categorie di interessati …….. pag 7
   4.5 Categorie di dati trattati ……pag. 7
   4.6 Accesso ai dati ……pag. 9
   4.7 modalità di raccolta e conservazione dei dati: strumenti e tecnologie utilizzati……pag. 9
5. PRINCIPI FONDAMENTALI……pag. 10
   5.1 Basi giuridiche che rendono lecito il trattamento dei dati…… ……pag. 10
   5.2 Periodo di conservazione dei dati ……:::……pag. 11
6. MISURE A TUTELA DEGLI INTERESSATI ……pag. 11
   6.1 Modalità di informazione degli interessati ……pag 11
   6.2 Modalità di esercizio degli interessati……pag 12
7. RISCHI……pag. 12
   7.2 Misure tecniche esistenti o pianificate……::……pag. 13

7.2 TABELLA DEI RISCHI AFFERENTI ALLA DPIA ……pag. 14

VALUTAZIONE CONCLUSIVE ……pag. 19

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 NECESSITÀ 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. Nel caso di specie, il trattamento in esame impatta su due criteri proposti dall'EDPB: con la Piattaforma vengono, infatti, trattati dati personali particolari di cui all'art. 9 del GDPR (**criterio 4**) di soggetti vulnerabili (**criterio 7**). 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, in qualità di Titolare del Trattamento, e Promotore dello studio clinico, ha predisposto la presente DPIA nella quale sono analizzati i rischi connessi al trattamento dei Dati Personali raccolti nell'ambito dello studio nazionale - multicentrico - osservazionale non farmacologico - retrospettivo dal titolo "La asimmetria delle lesioni endometriosiche come dimostrazione della teoria del reflusso mestruale e delle nicchie anatomiche: studio multicentrico italiano del gruppo ETIC" (acronimo: NICCHIENDO).

In base all'art. 110 Bis IV Comma del Codice, come recentemente ricordato dal Garante della Protezione dei Dati Personali nelle FAQ pubblicate in data 06.06.2024 in materia di "*Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca*" nel caso in cui gli IRCCS "*fondino il trattamento dei dati raccolti per finalità di cura per ulteriori finalità di ricerca sull'art. 110-bis, comma 4 del Codice, essi devono obbligatoriamente svolgere e pubblicare la Valutazione d'impatto (VIP), sui propri siti web, in quanto tale articolo costituisce una di quelle disposizioni di legge alle quali fa riferimento l'art. 110 del Codice, prescrivendo tali ulteriori adempimenti*".

Tale disposizione trova applicazione in relazione ad ogni tipo di ricerca medica, biomedica, epidemiologica, prospettica e retrospettiva, promossa da tali istituti ivi inclusi gli studi multicentrici, sia svolti nell'ambito delle reti di ricerca degli IRCCS che in quelli multicentrici promossi da tali istituti con la partecipazione di enti che non godono di tale riconoscimento.

Alla luce di quanto sopra, per la conduzione dello studio in oggetto, il Promotore intende ora predisporre una valutazione di impatto.

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 IRCCS**") per la conduzione dello studio dal titolo "*Asimmetria delle lesioni endometriosiche come dimostrazione della teoria del reflusso mestruale e delle nicchie anatomiche: studio multicentrico italiano del gruppo ETIC"*. I dati personali – così come definiti dall'art. 4.1) del GDPR – diversi dai Dati Personali, saranno indicati con le iniziali minuscole.

I Dati Personali, relativi alla diagnosi istologica, verranno raccolti dalle cartelle cliniche.

Database Dati Personali: l'insieme delle eCRF specifiche dello Studio salvate sulla piattaforma REDCap nelle quali sono salvati i Dati Personali.

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 nazionale - multicentrico - osservazionale non farmacologico - retrospettivo dal titolo "*Asimmetria delle lesioni endometriosiche come dimostrazione della teoria del reflusso mestruale e delle nicchie anatomiche: studio multicentrico italiano del gruppo ETIC*" volto a valutare la distribuzione asimmetrica delle lesioni endometriosiche a carico di organi pari e simmetrici, al fine di confermare la teoria del reflusso mestruale e la "anatomical niches hypotesis".

Interessati: i soggetti arruolati nello Studio a cui i Dati Personali si riferiscono. In particolare, verranno reclutate tutte le pazienti con diagnosi istologica di endometriosi e di endometriosi associata a carcinoma endometrioide, carcinoma a cellule chiare e tumore borderline sieromucinoso operate presso la Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico e presso i centri partecipanti allo studio dal 01/2013 al 12/2023.

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

3. DESCRIZIONE DEL TRATTAMENTO

4.1 Finalità del trattamento

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

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

Fondazione IRCCS in qualità di Promotore intende condurre uno studio clinico volto a valutare la distribuzione asimmetrica delle lesioni endometriosiche a carico di organi pari e simmetrici, al fine di confermare la teoria del reflusso mestruale e la "anatomical niches hypotesis".
Lo Studio intende validare la teoria del reflusso mestruale e delle nicchie anatomiche nell'eziopatogenesi dell'endometriosi.
Non sono previste visite e valutazioni cliniche. I dati verranno raccolti dalle cartelle cliniche della Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico e degli altri Centri partecipanti allo studio.
Verranno reclutate tutte le pazienti con diagnosi istologica di endometriosi e di endometriosi associata a carcinoma endometrioide, carcinoma a cellule chiare e tumore borderline sieromucinoso operate presso la Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico e presso i centri partecipanti allo studio dal 01/2013 al 12/2023.
In base al numero di donne trattate annualmente da parte del Centro promotore e dei Centri partecipanti allo studio, stimiamo che includere tutte le pazienti operate per endometriosi, per carcinoma endometrioide e a cellule chiare e per tumori borderline sieromucinosi nel periodo 20132023 consentirà di raggiungere la numerosità prevista.

4.2 Responsabilità connesse al trattamento

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

Titolare del trattamento: **Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico** in qualità di Promotore dello Studio clinico e Centro Coordinatore è titolare per la raccolta dei dati e per la gestione degli stessi nell'ambito dello Studio clinico.

I singoli centri partecipanti, di seguito elencati, agiranno in qualità di autonomi titolari del trattamento:

- Ospedale Borgo Roma
- Ospedale Santa Maria Annunziata
- Policlinico Umberto I
- Ospedale San Raffaele
- Policlinico Duilio Casula
- Policlinico Santa Maria alle Scotte,
- Ospedale San Giovanni Addolorata
- IRCCS Azienda Ospedaliero - Universitaria di Bologna - Policlinico di Sant'Orsola
- Ospedale Macedonio Melloni
- ARNAS Civico di Palermo
- Azienda Pugliese Ciaccio di Catanzaro
- Presidio Ospedaliero Universitario "Santa Maria della Misericordia", Azienda Sanitaria Universitaria Friuli Centrale
- Azienda Ospedaliero-Universitaria Maggiore della Carità di Novara

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), nonché il Provvedimento n. 146 del 5 giugno 2019. I Dati personali verranno trattati per la conduzione dello Studio in base all'art. 110 bis IV comma del Codice.

4.4 Categorie di interessati

a. Verranno reclutate tutte le pazienti con diagnosi istologica di endometriosi e di endometriosi associata a carcinoma endometrioide, carcinoma a cellule chiare e tumore borderline sieromucinoso operate presso la Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico e presso i centri partecipanti allo studio dal 01/2013 al 12/2023. Criteri di inclusione:
   età <18 anni - pazienti affette da carcinoma endometrioide o a cellule chiare Stadio I-II o tumore ovarico borderline sieromucinoso non associati a endometriosi o in stadio di malattia più avanzato - donne con diagnosi ecografica di endometriosi non sottoposte a chirurgia - precedenti interventi per endometriosi eseguiti presso altro centro
b. ricercatori e altro personale del Titolare coinvolti nello Studio.

4.5 Categorie di dati trattati

(Elencare i dati raccolti e trattati indicando il periodo di conservazione, i destinatari e le persone che possono accedervi)

I dati relativi alla diagnosi istologica verranno raccolti dalle cartelle cliniche. In particolare, ci focalizzeremo sulle pazienti con diagnosi istologica di:

1. endometriosi ovarica (sia primari che recidive dopo intervento)

2. endometriosi del colon ascendente e/o discendente (al fine di avere una diagnosi certa ed uniforme tra i vari Centri, verranno considerati solamente i casi severi condizionanti stenosi e sottoposti a chirurgia, esclusa localizzazione isolata dell'appendice)

3. endometriosi ureterale (al fine di avere una diagnosi certa ed uniforme tra i vari Centri, verranno considerati solamente i casi severi condizionanti idroureteronefrosi e sottoposti a chirurgia) e vescicale

4. endometriosi del nervo sciatico (visualizzata chirurgicamente o tramite RMN)

5. endometriosi inguinale-legamento rotondo

6. endometriosi dei legamenti utero-sacrali

7. endometriosi peritoneale

8. endometriosi diaframmatica-epatica

9. endometriosi pleurica e polmonare (visualizzata chirurgicamente o tramite TC)

10. endometriosi ombelicale (associata a emidraframma destro e/o emidiaframma sinistro)

11. carcinoma endometrioide e a cellule chiare al I-II stadio 12. tumori ovarici borderline sieromucinosi

4.6 Accesso ai dati

Soggetti che accedono ai Dati Personali

L'accesso ai Dati Personali è consentito a:

1) Sperimentare Principale

2) Ricercatori che supportano lo Sperimentatore Principale nella conduzione dello studio

3) Sperimentatori locali e Ricercatori che supportano lo Sperimentatore locale nella conduzione dello studio

4.7 modalità di raccolta e conservazione dei dati: strumenti e tecnologie utilizzati

I dati necessari per lo studio verranno registrati in una apposita eCRF in un Data Management System validato 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. La CRF verrà compilata dal Prinicipal Investigator dello Studio a (o suo delegato) che deve verificare che ogni dato.

4. PRINCIPI FONDAMENTALI

5.1 Basi giuridiche che rendono lecito il trattamento dei dati

Ai sensi dell'art. 110 bis IV comma del Decreto 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.

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 25 ANNI, in conformità a quanto stabilito dal Regolamento UE 2014/536.

5. MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

6.1 Modalità di informazione degli interessati

Per i pazienti del gruppo A:

non verrà chiesto alcun consenso per la partecipazione al presente studio né per il trattamento dei dati personali poiché saranno arruolati in maniera retrospettiva. Stante la natura di Istituti di Ricovero e Cura a

Carattere Scientifico del Policlinico, promotore dello studio, in conformità alla normativa vigente in materia di tutela e protezione dei dati personali (Reg. UE 679/2016) e D.Lgs196/2003 (Codice della Privacy) come novellato dal D.Lgs 101/2018, non verrà richiesto ai pazienti del gruppo B un consenso all'utilizzo dei propri dati personali per la conduzione dello studio stesso. In conformità a quanto disposto dall'art. 110 bis comma IV del novellato D.Lgs 196/2003, in ragione del carattere strumentale che l'attività di assistenza sanitaria assume rispetto alla ricerca presso gli Istituti di Ricovero e Cura a Carattere Scientifico, il trattamento, per finalità di ricerca, di dati personali già raccolti per attività clinica, compresa la anonimizzazione degli stessi, non costituisce ulteriore trattamento. Pertanto, lo studio in oggetto ha natura osservazionale e retrospettiva e, in quanto tale, prevede l'utilizzo di dati raccolti in precedenza per attività di cliniche, il suddetto utilizzo, non costituendo un nuovo trattamento (come specificato dal dettato normativo), non richiede l'espressione di un nuovo consenso da parte degli interessati che hanno già espresso il loro consenso per l'utilizzo dei propri dati per attività clinico-assistenziali. Non sarà pertanto presentata loro la informativa al trattamento dati, richiesta dall'art. 13 del D.Lgs.196/2003. Resta inteso che il trattamento dei dati avverrà nel rispetto delle garanzie previste per tutelare i diritti e le libertà dell'interessato, in conformità a quanto disposto dall'art. 89 del Codice della privacy. Tali garanzie comprendono l'adozione di misure tecniche e organizzative al fine di garantire il rispetto del principio dell'anonimizzazione dei dati, tra cui la pseudonimizzazione e la pubblicazione sul sito web della presente valutazione di impatto e della informativa al trattamento dati.

Ove applicabile: come si ottiene il consenso degli interessati?

N.A.

6.2 Modalità di esercizio dei diritti degli interessati

I soggetti interessati potranno esercitare i loro diritti scrivendo:

- all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy dell'Istituto, reperibile sia nell'informativa generale che nel sito web istituzionale;
- direttamente presso il P.I. 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. L'istituto 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:

a. Anonimizzazione

N.A. I Dati Personali non vengono anonimizzati in quanto non sarebbero più utilizzabili per la conduzione dello Studio

b. Crittografia

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).

c. Controllo degli accessi

Le credenziali di accesso al Database sono studio specifiche e vengono fornite solo agli Sperimentatori principali e al personale autorizzato dalla Fondazione IRCCS e dai Centri Partecipanti 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;
- impegno dei Centri Partecipanti a richiedere, senza ritardo, la disattivazione di utenze non più necessarie;
- 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.

Per aumentare il livello di sicurezza verrà implementata, anche per i Soggetti arruolatori e altro personale autorizzato dai Centri Partecipanti nell'ambito dello Studio, l'autenticazione a 2 fattori, ma basata sull'utilizzo di codici verifica che saranno inviati alle e-mail istituzionali degli utenti.

d. Tracciabilità

Tutte le attività compiute dai Centri Partecipanti arruolanti e/o dagli altri utenti sono registrate mediante file di log. REDCap ha un sistema di log interno che registra automaticamente tutte le attività degli utenti e tutte le pagine viste da ogni utente, comprese le informazioni contestuali (ad esempio lo studio o il record a cui si accede). REDCap registra tutte le azioni quali, per esempio, le attività di inserimento di dati, esportazione di dati, modifica di un campo, esecuzione di un report o aggiunta/modifica di un utente, tra una pletora di altre attività. Il record di registrazione può essere visualizzato all'interno di uno spazio dedicato solo dagli Amministratori di Sistema. La pagina di registrazione permette a tali utenti di visualizzare i log completi dello studio, e anche di filtrarli in vari modi in base al tipo di attività e/o utente. Il log interno di REDCap permette agli amministratori di essere in grado di determinare tutte le attività e tutti i dati visti o modificati da qualsiasi

utente; in particolare, i log verranno conservati per un periodo di 3 (tre) mesi dal termine dello Studio. Tutti i log sono memorizzati all'interno del database Mysql.

I Sistemi/Applicativi registrano i log degli accessi degli utenti e delle operazioni eseguite. In particolare, viene registrato: il tipo di evento, il successo o il fallimento, l'ora in cui è avvenuto l'evento, account coinvolto, processi coinvolti (come ad esempio, login/logout eseguiti e falliti, aggiunte, modifiche, cancellazioni dell'account, attribuzione di privilegi all'utente, aggiunte e modifiche ai parametri di log di sicurezza/controllo, switch degli username durante una sessione online, attività eseguite dagli account con privilegi elevati nel rispetto di quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008).

e. Archiviazione

Archiviazione informatica:

- Il database è strutturato in cluster e vengono effettuati backup giornalieri.
- Il database Mysql è fornito mediante il servizio di gestione Amazon Relational Database Services (RDS). Esso permette di automatizzare le attività di gestione del database (provisioning, configurazione, backup automatico, aggiornamento). Amazon RDS offre un elevato livello di sicurezza per i database MySQL. Sono, inoltre, adottate le seguenti misure l'isolamento di rete tramite Amazon Virtual Private Cloud (VPC), la crittografia dei dati inattivi tramite chiavi create e controllate tramite AWS Key Management Service (KMS) e la crittografia dei dati in transito tramite SSL.
- Tutte le macchine virtuali sono sottoposte a backup giornaliero mediante procedure automatiche di AWS (AWS backup) e Aruba (backup eVault).
- Su AWS in ogni momento è possibile duplicare l'infrastruttura in un'altra region di AWS a partire da questi snapshot (disaster recovery).
- I dischi di tutte le macchine e tutti i backup sono criptati (encryption at rest).
- Lo SLA relativo all'accesso ai dati di backup è pari al 99.9% mensile.
- 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).

Archiviazione Cartacea:

L'archiviazione sicura della documentazione cartacea (sottochiave con accesso limitato alle sole persone autorizzate) è rimessa alla responsabilità dei singoli centri Partecipanti e della Fondazione IRCCS.

f. Minimizzazione

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.

g. Vulnerabilità

Almeno una volta all'anno viene eseguito un test di vulnerabilità e penetrazione per verificare la sicurezza del sistema, eventuali vulnerabilità verranno corrette mettendo il sistema in sicurezza.

Duplicazione dei dati:

- Il database è strutturato a cluster e vengono effettuati backup giornalieri.

La Piattaforma REDCap implementa le seguenti misure di sicurezza:

- 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.
- L'utente è forzatamente obbligato all'utilizzo di una password che contenga almeno 10 caratteri, che abbia almeno tre delle seguenti 4 categorie:
    - carattere Maiuscolo;
    - carattere Minuscolo;
    - un numero tra 0 e 9;
    - carattere Speciale (!#@[] ecc.).

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.

h. Gestione degli incidenti di sicurezza e le violazioni dei dati personali

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.

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 integrità	Improbabile, in base alle misure implementate e pianificate, si stima una limitata probabilità di verificarsi del rischio.	Trascurabile	Molto Basso	Partizionamento, Tracciabilità, Controllo degli accessi logici, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Backup, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestione dei rischi, Protezione contro fonti di rischio non umane, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Controllo degli accessi fisici, Archiviazione, Crittografia, Vigilanza sulla protezione dei dati, Politica di tutela della privacy.
Perdita di disponibilità	Improbabile, in base alle misure implementate e pianificate, si stima una limitata probabilità di verificarsi del rischio.	Trascurabile	Molto Basso	Backup, Archiviazione, Partizionamento, Tracciabilità, Controllo degli accessi logici, Controllo degli accessi fisici, Minimizzazione dei dati, Vulnerabilità, Crittografia, Lotta contro il malware, Gestione postazioni, Gestione dei rischi, Gestione del personale, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati.
Accesso ai dati non autorizzato	Improbabile, in base alle misure implementate e pianificate, si stima una limitata probabilità di verificarsi del rischio.	Trascurabile	Molto Basso	Lotta contro il malware, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Minimizzazione dei dati, Gestione del personale, Vulnerabilità, Archiviazione, Tracciabilità, Crittografia, Partizionamento, Controllo degli accessi fisici, Gestione dei rischi, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Formazione degli autorizzati al trattamento, Controllo degli accessi logici.

Trattamento non autorizzato	Poco probabile	Marginali	Basso	Controllo della eCRF e delle abilitazioni preventivo alla massa in produzione da parte dell'amministratore di sistema, policy legate alla gestione e controllo delle utenze: accesso limitato alla visualizzazione al singolo utente, formazione periodica degli operatori sul tema
Trattamento non conforme alla finalità o illecito	Probabile	Limitate	Medio	Controllo delle eCRF preventivo alla messa in produzione dell'amministratore di sistema, policy aziendale di compliance al GDPR, formazione periodica degli operatori sul tema, istruzioni operative specifiche.

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

Valutazioni conclusive

Opinione degli interessati o dei loro rappresentanti (ove raccolta)
Parere del Responsabile Protezione Dati (DPO)
Stante l'ente il basso livello di rischio individuato per il trattamento dei dati oggetto dello studio e le misure adottate, si ritiene che la conduzione dello Studio NICCHIENDO non comporti problematiche. Pertanto, si ritiene accettabile la modalità di trattamento.

Validazione della DPIA

Sottoscrizioni	**Firma**	**Data**
Il Responsabile Protezioni dati		
Il Principal Investigator dello Studio		
Il Titolare del trattamento	Firmato da: FABIO BLANDINI Codice fiscale: BLNFBA62E02F158S Valido da: 01-06-2022 14:03:12 a: 01-06-2025 01:00:00 Certificato emesso da: InfoCert Qualified Electronic Signature CA 3, InfoCert S.p.A., IT Riferimento temporale 'SigningTime': 04-12-2024 12:30:08 Approvo il documento	

Aggiornamenti successivi:

Data	Aggiornamento