SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI COMPREHENSIVE Cancer Centre

Infrastruttura Ricerca e Statistica

# Implementazione e utilizzo di REDCap per la raccolta e gestione dei dati personali per scopo di ricerca. Valutazione d'Impatto sulla Protezione dei Dati (DPIA) AUSL-IRCCS di Reggio Emilia

Sommario



IRCCS Istituto in Tecnologie Avanzate e
Modelli Assistenziali in Oncologia
Ex Ospedale Spallanzani
Viale Umberto I°, 50 – 42123 Reggio Emilia
T. +39.0522.295.620 – Fax +39.0522.285.622
elisa.mazzini@ausl.re.it

**Sede Legale**: Via Amendola, 2 - 42122 Reggio Emilia
T. +39.0522.335.111 – Fax +39.0522.335.205
C.F. e Partita IVA 01598570354
www.ausl.re.it

## 1. Identificazione del progetto

| | |
|---|---|
| Nome del Progetto | Implementazione e utilizzo di REDCap per la raccolta e gestione dei dati personali per scopo di ricerca. |
| Titolare Trattamento | AUSL-IRCCS di Reggio Emilia |
| Responsabile Trattamento | Biomeris SRL |
| Responsabile elaborazione DPIA | • Eleonora Ferretti<br>Responsabile S.S. Clinical Trial Center<br>Infrastruttura Ricerca e Statistica<br>AUSL IRCCS di Reggio Emilia<br>• Biomeris SRL |
| Responsabile della protezione dei dati (DPO) | • Erica Molinari |

## 2. Premessa

La raccolta accurata dei dati è fondamentale per la validità e l'affidabilità dei risultati di uno studio o progetto di ricerca. Per tale motivo è importante avvalersi di uno strumento in grado di garantire l'integrità e la qualità del dato.
REDCap (Research Electronic Data Capture) è un sistema di gestione di dati elettronici (Electronic Data Capture -EDC) sviluppato originariamente presso la Vanderbilt University a disposizione della comunità scientifica.
Di seguito si riassumono le caratteristiche più significative della piattaforma.

## 3. Effettuazione della Valutazione di impatto sulla protezione dei dati (DPIA) al trattamento dei dati per scopo di ricerca mediante REDCap

Visto l'articolo 35 del GDPR il quale stabilisce che “Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali”, si ritiene che sussistano le condizioni per provvedere alla effettuazione della DPIA relativamente al trattamento dei dati personali effettuato mediante l’applicativo REDCap, sistema di gestione di dati clinici e di ricerca, in quanto il trattamento dei dati per finalità di ricerca rientra nei casi in cui la DPIA è obbligatoria e in quanto prevede un trattamento di dati di natura particolare, eventualmente condivisi tra più titolari, ai sensi sia del wp248 rev.01 del 4/10/2017 recante “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”, sia dell’Allegato 1 al Provvedimento del Garante n. 467/2018, recante “Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d’impatto”, con particolare riferimento alle tipologie nn. 3, 4, 6, 7, 8, 10;

## 4. Descrizione del Progetto

### *4.1 Descrizione del trattamento dei dati*

REDCap è una piattaforma utilizzata per la raccolta e la gestione dei dati personali per scopi di ricerca. È utilizzato per raccogliere e gestire dati clinici strutturati (dati numerici e alfanumerici) e non strutturati (note cliniche, file allegati come immagini mediche o referti) provenienti da studi clinici, survey e progetti di ricerca.

Il trattamento dei dati personali e dei dati particolari può includere, se e in quanto rilevanti per lo studio:

- **Dati personali:** età, sesso, stato civile, occupazione, area di residenza;
- **Dati sanitari/clinici**: diagnosi, terapie in corso, anamnesi, esami clinici, trattamenti farmacologici, esiti di esami di laboratorio, esiti di visite cliniche specialistiche, ecc.;
- **Dati biometrici o genetici**;
- **Dati relativi al consenso informato**: informazioni su quando e come il consenso informato e il consenso al trattamento dei dati sono stati ottenuti;
- **Dati socio economici**: titolo di studio, situazione lavorativa, reddito, situazione familiare, ecc.;

Tutti i dati raccolti in REDCap sono pseudonimizzati: i dati identificativi dei pazienti arruolati vengono conservati a cura del PI nella patient identification list. Inoltre, i dati trattati sono sempre esclusivamente nella disponibilità della Azienda e rimangono archiviati in modo sicuro nei sistemi aziendali.

La piattaforma REDCap è installata in una *Virtual Private Cloud* ospitata su datacenter europei di AWS. L'account AWS, di proprietà di BIOMERIS SRL, è dedicato esclusivamente all'uso dell'Azienda USL IRCCS di Reggio Emilia.

### *4.2 Finalità del trattamento*

L'obiettivo principale è raccogliere e gestire dati per scopo di ricerca in modo sicuro ed efficiente, migliorando l'accessibilità e l'integrità dei dati rispetto ai sistemi cartacei.
In sintesi, le finalità principali possono includere:

a) **Ricerca clinica**, ovvero gli studi scientifici che coinvolgono direttamente i pazienti o i volontari umani per valutare l'efficacia, la sicurezza e i benefici di trattamenti, farmaci, dispositivi medici o interventi diagnostici e terapeutici al fine di migliorare la cura dei pazienti, sviluppando nuove terapie o testando nuove applicazioni di trattamenti esistenti. Le principali tipologie di ricerca clinica includono:
   - *Studi sperimentali (trial clinici):* si conducono per testare interventi in condizioni controllate.
   - *Studi osservazionali:* si osservano i pazienti senza interventi diretti per raccogliere dati e analizzare risultati clinici.

**b)** **Ricerca sanitaria** ovvero gli studi scientifici volti a migliorare la salute e il benessere della popolazione. Essa può comprendere studi non direttamente focalizzati su interventi clinici, ma su questioni più generali legate ai sistemi sanitari, alle politiche pubbliche, alla

prevenzione delle malattie, alla promozione della salute e alla gestione delle risorse sanitarie. La ricerca sanitaria può riguardare:

- *Studi sui determinanti sociali e ambientali della salute:* Come l'educazione, l'ambiente di lavoro e il contesto sociale influenzano la salute.
- *Ricerca sulle politiche sanitarie:* Analisi di come le leggi, le normative e le politiche influenzano l'accesso e la qualità delle cure.
- *Ricerca in ambito di salute pubblica:* Studi sulla prevenzione delle malattie, la gestione delle pandemie e il miglioramento della salute della comunità.

## *4.3 Modalità di trattamento*

### 4.3.1 Raccolta dei dati

I dati clinici e di ricerca, una volta pseudonimizzati a cura del PI, vengono raccolti tramite moduli elettronici personalizzati progettati *ad hoc* per studi clinici, survey e progetti di ricerca.
Questi moduli sono compilati da personale autorizzato (medici, infermieri, CRC, ricercatori).
I campi nei moduli possono essere obbligatori o facoltativi e programmati per raccogliere solo dati rilevanti ai fini dello studio.
La raccolta dei dati avviene su una connessione sicura (HTTPS) con certificati SSL per garantire la protezione durante la trasmissione dei dati.
I dati vengono crittografati sia in transito che a riposo sui server che ospitano REDCap, riducendo il rischio di accesso non autorizzato.

### 4.3.2 Accesso e autorizzazioni

REDCap utilizza un sistema di controllo degli accessi basato su ruoli per garantire che solo il personale autorizzato possa accedere ai dati. Ogni utente ha un ruolo specifico (es. data entry, monitor, sperimentatore, revisore, amministratore) che definisce i permessi di lettura, scrittura e modifica. Il ruolo viene concordato con il PI dello studio e assegnato dal personale addetto del CTC in accordo al protocollo di ricerca e al contratto per la conduzione dello studio.
Gli utenti accedono alla piattaforma tramite credenziali uniche (username e password). REDCap è stato implementato con un sistema di autenticazione a 2 fattori (2FA), basato sull'utilizzo di codici verifica per garantire che solo utenti autorizzati possano accedere ai dati.
Tutte le operazioni eseguite dagli utenti vengono tracciate tramite un audit log che registra data, ora e azioni intraprese (es. accesso, modifica dei dati, esportazione).
Oltre al personale dell'AUSL RE IRCCS autorizzato al trattamento, anche il personale di altre strutture pubbliche o private coinvolte nei singoli studi clinici potrà avere accesso ai dati in accordo con quanto specificato nel protocollo e nel contratto per la conduzione dello studio.

Per quanto riguarda la gestione delle credenziali l'istanza REDCap in uso utilizza un metodo di autenticazione interno basato su tabelle, che prevede la creazione della password da parte dell'utente finale mediante link inviato via email al momento dell'attivazione dell'utenza. La password risponde alle seguenti caratteristiche/misure di sicurezza.

- Lunghezza: 9 caratteri
- Complessità: Almeno una lettera maiuscola, una minuscola e un numero
- Durata: 90 giorni

- Non è possibile riutilizzare le 5 password più recenti
- Dopo 5 tentativi di inserimento falliti, l'utente viene bloccato per 15 minuti
- La compilazione automatica della password è disabilitata.

### 4.3.3 Trasferimento e condivisione dei dati

I dati raccolti tramite REDCap possono essere esportati per analisi o revisione esterna. Tutte le esportazioni avvengono in modalità sicura. I dati possono essere esportati in forma pseudonimizzata ma, in fase di esportazione possono anche essere anonimizzati per ridurre il rischio di identificazione diretta dei soggetti.
La funzione di esportazione dati è sotto la responsabilità del Clinical Trial Center (CTC) che assegna la funzione di esportazione allo Statistico individuato dal protocollo di studio/ricerca.
I dati possono anche essere trasferiti o condivisi con terze parti, in conformità a specifici accordi contrattuali. In tal caso, gli interessati del trattamento dovranno essere informati e autorizzare tale trasferimento/condivisione.

I dati vengono trasferiti attraverso connessioni sicure (SFTP, HTTPS) o scaricati localmente in formato crittografato, assicurando che la privacy sia preservata durante il trasferimento.
La piattaforma REDCap consente di condividere i dati solo con utenti o partner autorizzati e i permessi di condivisione sono configurati in base al ruolo dell'utente. È possibile impostare restrizioni per garantire che solo i dati strettamente necessari vengano condivisi.

### 4.3.4 Archiviazione e conservazione dei dati

I dati raccolti tramite REDCap vengono archiviati in un ambiente sicuro e crittografato. Il server che ospita REDCap è configurato in un'infrastruttura cloud sicura conforme agli standard di protezione dei dati (ISO 27001, HIPAA, ecc.).

I backup sono eseguiti regolarmente per garantire la continuità operativa e la protezione in caso di guasto o incidente. Il backup dell'istanza viene effettuato prima e dopo ogni attività di manutenzione.
Il backup dell'istanza database viene eseguito quotidianamente in modo automatico e mantenuto per 35 giorni.

Al termine dello studio il progetto configurato in REDCap viene passato allo stato di 'Completato', ovvero messo offline, rimosso dall'elenco dei progetti impedendone l'accesso. Questo garantisce che il progetto e i dati contenuti rimangano intatti ed accessibili per il periodo di conservazione definito dal protocollo di ricerca e dai requisiti normativi. Solo gli amministratori possono annullare il passaggio allo stato di 'Completo' e riportare il progetto ad uno stato accessibile.

I dati sono conservati per il periodo definito dal protocollo di ricerca o dai requisiti normativi. Dopo il termine di questo periodo, i dati possono essere cancellati in modo sicuro o resi anonimi in modo irreversibile, in conformità con le normative vigenti.

### 4.3.5 Minimizzazione e anonimizzazione dei dati

REDCap è configurato per raccogliere solo i dati necessari (minimizzazione dei dati) per gli scopi specificati nel progetto o nello studio. Questo approccio riduce il rischio di trattare informazioni non necessarie che potrebbero aumentare l'esposizione a rischi per la privacy.
La minimizzazione dei dati viene applicata tramite la riduzione del numero di dati identificativi raccolti e la raccolta di soli dati pseudonimizzati. In molti casi, REDCap permette di evitare del tutto la raccolta di informazioni personali che potrebbero identificare direttamente il soggetto, quando non strettamente necessario. Per esempio, i dati demografici o clinici possono essere raccolti in forma aggregata o con dettagli ridotti (es. intervalli di età piuttosto che età esatta, aree geografiche generali anziché indirizzi specifici).

A seconda delle esigenze del progetto, i dati possono essere raccolti in forma anonima all'interno di REDCap.

#### 4.3.6 Eliminazione sicura dei dati

Al termine dello studio o del progetto, in accordo al protocollo e al periodo dichiarato di conservazione i dati non più necessari potranno essere:

a. eliminati in modo sicuro seguendo le linee guida di cancellazione fornite dalle normative di protezione dei dati. REDCap consente la cancellazione permanente dei dati tramite metodi sicuri, evitando il rischio di recupero successivo.
b. anonimizzati in modo tale che non possano più essere attribuiti a un soggetto specifico senza ulteriori informazioni. Una volta anonimizzati in maniera adeguata, i dati, non più soggetti alle stesse restrizioni delle normative privacy, potranno essere conservati e utilizzati per scopi di ricerca di analisi statistica o potranno essere ceduti a Terzi.

#### 4.3.7 Misure di sicurezza aggiuntive

Oltre alla crittografia standard durante la trasmissione e l'archiviazione, REDCap può essere configurato per garantire che determinati campi sensibili siano ulteriormente protetti con livelli aggiuntivi di crittografia.
Il personale che utilizza REDCap riceve una formazione regolare sulla gestione sicura dei dati e sulle normative vigenti in materia di protezione dei dati.

### *4.4 Durata del trattamento*

I dati saranno conservati in accordo al protocollo di studio o comunque per il tempo previsto dalla normativa applicabile, al termine del quale i dati saranno distrutti o completamente anonimizzati.

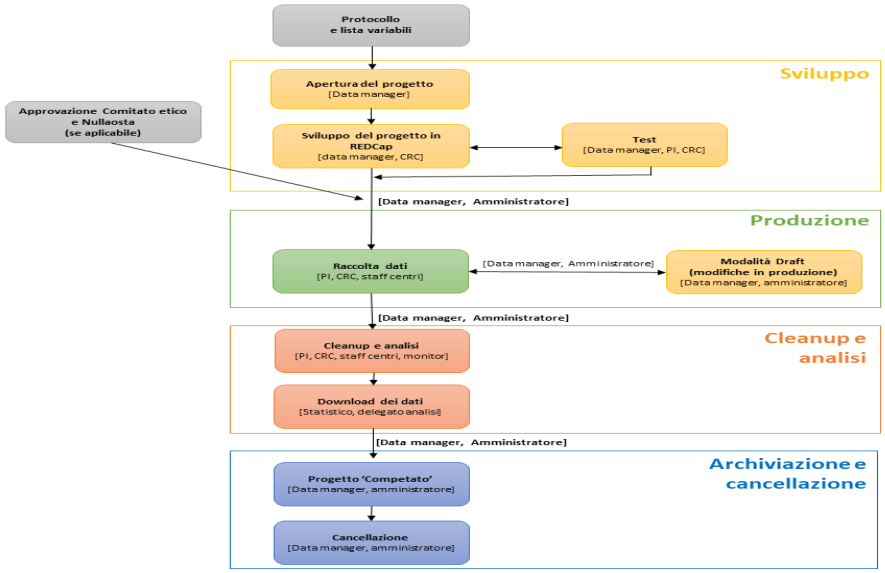
### *4.5 Installazione, manutenzione ed interruzioni del servizio*

Il codice sorgente di REDCap è fornito gratuitamente dalla Vanderbilt University a enti accademici e no-profit. Per scaricare il codice sorgente direttamente dall'area riservata del sito ufficiale del REDCap Consortium, è stato necessario firmare un accordo di licenza con la Vanderbilt University. Il software scaricato è stato condiviso con BIOMERIS SRL per l'installazione e la configurazione sul server dedicato. L'area riservata del REDCap Consortium offre inoltre un accesso continuo agli

aggiornamenti e agli sviluppi del software, con descrizioni dettagliate delle modifiche apportate, delle problematiche riscontrate e la possibilità di scaricare le nuove release.
Le attività di manutenzione ordinaria e straordinaria del server e dell'applicativo sono gestite da BIOMERIS SRL per conto dell'Azienda USL IRCCS di Reggio Emilia. A tal fine BIOMERIS SRL viene designata dalla Ausl di Reggio Emilia-IRCCS quale Responsabile del trattamento ai sensi dell'art. 28 GDPR
Le attività di manutenzione ordinaria che richiedono interruzioni del servizio verranno pianificate con largo anticipo e comunicate a tutti gli utenti attivi via e-mail almeno 15 giorni prima. In caso di interventi urgenti, la sospensione del sistema verrà comunque notificata agli utenti, cercando di fornire un preavviso se possibile, anche minimo.
Il tempo di intervento sarà limitato al minimo indispensabile, mantenendo il sistema offline il minor tempo possibile per garantire la continuità del servizio agli utenti. Durante la sospensione del servizio il sistema inizialmente viene messo offline per avvisare gli utenti che non possono utilizzare la piattaforma durante il ripristino e successivamente viene reso irraggiungibile durante le operazioni di aggiornamento.
Nel caso di interruzione inaspettata superiore alle 8 ore, tale interruzione verrà segnalata agli utenti mediante e-mail dal CTC, insieme ad eventuali informazioni rispetto ai tempi di ripristino. Non appena il sistema verrà ripristinato ne verrà data comunicazione agli utenti attivi. I tempi di risposta concordati in fase di contratto con BIOMERIS SRL sono 24 ore per le problematiche bloccanti e 72 ore per le situazioni non bloccanti.

### 4.5.1 Fasi di Sviluppo dei Progetti su REDCap

Lo studio clinico, survey o progetto di ricerca si configura in REDCap come un "Progetto". Ogni progetto si articola in uno o più moduli che raccolgono i dati dello studio, survey o progetto di ricerca.



## 5. Valutazione della necessità e proporzionalità

### *5.1 Necessità del trattamento*

La raccolta del dato in uno studio clinico è elemento fondamentale per produrre risultati attendibili. L'integrità e la qualità del dato è garantita grazie all'aderenza dei principi ALCOA (Attributable, Legible, Contemporaneous, Original, Accurate) come richiesto dalle GCP (Good Clinical Practice) e dalle Autorità Competenti (FDA, EMA).

REDCap garantisce l'aderenza ai criteri ALCOA e ALCOA++. La piattaforma offre strumenti e funzionalità per garantire che i dati siano attribuibili, leggibili, contemporanei e accurati, contribuendo così a rispettare i requisiti di integrità dei dati in contesti regolamentati e scientifici

| | | |
|---|---|---|
| Attributable (Attribuibile) | Ogni dato raccolto deve essere attribuibile a una persona o un sistema che lo ha generato. È essenziale sapere chi ha raccolto o modificato i dati e quando ciò è avvenuto. | ○ REDCap utilizza un sistema di accesso basato su utenti autenticati (*username e password)* che permette di tracciare chi ha inserito o modificato i dati.<br>○ Ogni operazione effettuata dagli utenti (inserimento, modifica, cancellazione) viene registrata in un *audit trail***.** Questo audit log include informazioni su chi ha eseguito l'azione, quando è stata fatta e quali dati sono stati modificati.<br>○ L'accesso e le autorizzazioni possono essere configurati in base ai ruoli degli utenti, assicurando che solo il personale autorizzato possa inserire, visualizzare o modificare determinati dati. |
| **Criterio** | Descrizione | REDCap |
| Legible (Leggibile) | I dati devono essere facilmente leggibili e comprensibili anche a distanza di tempo. | ○ I dati sono inseriti tramite interfacce standardizzate e strutturate che permettono di raccogliere informazioni in formati leggibili e coerenti.<br>○ I moduli di REDCap possono essere progettati per garantire che i dati siano presentati in modo chiaro e ordinato, con campi predefiniti, menù a tendina e selettori che minimizzano errori e dati illeggibili.<br>○ I dati storici o modificati rimangono accessibili in forma leggibile attraverso l'audit log, rendendo possibile la revisione completa di eventuali cambiamenti apportati ai dati. |
| Contemporaneous (Contemporaneo) | I dati devono essere registrati nel momento in cui si verificano o il più vicino possibile al momento dell'evento. | ○ REDCap permette l'inserimento dei dati in tempo reale durante la raccolta, garantendo che siano contemporanei agli eventi clinici o sperimentali.<br>○ I *timestamp* automatici registrano la data e l'ora di ogni inserimento o modifica dei dati, assicurando che le informazioni siano raccolte e tracciate nel momento corretto.<br>○ Per i progetti che richiedono l'acquisizione di dati retrospettivi, REDCap permette di registrare la data dell'evento in modo esplicito, differenziando chiaramente tra la data di raccolta e la data dell'evento. |
| Original (Originale) | I dati devono essere la registrazione originale o una | ○ I dati inseriti in REDCap sono considerati dati originali **solo** quando sono raccolti direttamente tramite la piattaforma. Questo avviene ad esempio |

| | | |
|---|---|---|
| | copia fedele dei dati originali (i cosiddetti "source data"). | nel caso di eCRF (moduli elettronici) compilati direttamente dai partecipanti allo studio.<br>○ L'*audit trail* in REDCap conserva tutte le modifiche effettuate sui dati, permettendo di confrontare le versioni successive con il dato originale. |
| Accurate (Accurato) | I dati devono essere precisi, corretti e riflettere esattamente ciò che è stato osservato o misurato. | ○ REDCap utilizza una serie di strumenti di convalida dei dati, come validazioni di campo (es. controlli di formato, range numerici, obbligatorietà dei campi) che aiutano a garantire che i dati inseriti siano accurati e coerenti.<br>○ I dati vengono spesso inseriti direttamente dai medici o dal personale autorizzato, riducendo la possibilità di errori di trascrizione.<br>○ L'inserimento dei dati può essere ulteriormente controllato tramite revisioni manuali o funzionalità di doppio data entry**,** che confronta due inserimenti separati per verificarne la corrispondenza. |
| **Complete (Completo)**: | Tutti i dati rilevanti devono essere raccolti, senza omissioni. | ○ In REDCap, la completezza dei dati è supportata dall'uso di campi obbligatori e checklist che aiutano a garantire che tutte le informazioni necessarie siano raccolte. |
| **Consistent (Coerente)**: | I dati devono essere registrati in modo coerente e uniforme. | ○ La standardizzazione dei campi e dei moduli in REDCap garantisce che i dati siano raccolti in modo coerente per tutti i partecipanti allo studio anche se arruolati in centri diversi. |
| **Enduring (Duraturo)**: | I dati devono essere conservati in modo che rimangano accessibili e leggibili nel tempo. | ○ REDCap archivia i dati in modo sicuro e duraturo, con backup regolari e un accesso continuo garantito per la durata del progetto. |
| **Available (Disponibile)**: | I dati devono essere prontamente disponibili per la revisione o l'uso | ○ REDCap garantisce l'accessibilità dei dati ai ricercatori autorizzati in qualsiasi momento, con possibilità di esportazione per analisi o verifiche normative |

### *5.2 Proporzionalità*

REDCap consente la raccolta dei dati essenziali per lo studio, minimizzando la raccolta di dati non necessari grazie a una progettazione modulare basata sul progetto di ricerca o sullo studio clinico autorizzato dal Comitato Etico competente. La corrispondenza tra il dato richiesto dal progetto/studio e dal modulo REDCap disegnato per la raccolta è garantita da una verifica dal personale del CTC (Data Manager). Il progetto sviluppato in REDCap viene messo in produzione solo a seguito di esito positivo di tale verifica.

## 6. Identificazione e analisi dei rischi

| Rischio | Descrizione | Valore Iniziale | | | Misure di mitigazione (descritte in sezione 7) | Valore Residuo dopo le misure di mitigazione | | |
|---|---|---|---|---|---|---|---|---|
| | | I | P | R | | I | P | R |
| Accesso non autorizzato ai dati | Perdita di riservatezza dei dati personali coperti da segreto professionale; perdita del controllo dei propri dati; decifratura non autorizzata dei dati pseudonimizzati; diffusione dei dati non autorizzata | 4 | 2 | 8 | - Controllo degli accessi logici<br>- Tracciabilità<br>- Pseudonimizzazione<br>- Archiviazione<br>- Partizionamento<br>- Aggiornamento<br>- Crittografia.<br>- Revisione dei processi per la conformità GDPR e normativa vigente.<br>- Aggiornamento<br>- Monitoraggio continuo delle performance | 2 | 1 | 2 |
| Cancellazione/Perdita di dati | Una perdita dei dati potrebbe causare l'alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio; tuttavia non si tratta di dati originali | 2 | 2 | 4 | - Backup e ripristino<br>- Lotta contro malware<br>- Archiviazione<br>- Tracciabilità<br>- Controllo degli accessi logici<br>- Retention dei dati.<br>- Aggiornamento<br>- Protezione da vulnerabilità<br>- Monitoraggio continuo delle performance | 1 | 1 | 1 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Modifiche indesiderate | Perdita di integrità del dato; la modifica potrebbe essere definitiva e avere conseguenze sulla attendibilità dei risultati dello studio | 3 | 3 | 9 | - Gestione del personale<br>- Qualità dei dati<br>- Protezione da vulnerabilità<br>- Monitoraggio continuo delle performance | 2 | 2 | 4 |

| | | **Probabilità (P)** | **Impatto o Entità del Danno (I)** |
|---|---|---|---|
| 1 | molto bassa | accade solo in circostanze eccezionali (P < 5%) | insignificante |
| 2 | bassa | è improbabile che accada (5% < P < 20%) | bassa |
| 3 | media | può accadere in un certo numero di casi (20% < P < 50%) | moderata |
| 4 | alta | avviene in una buona parte dei casi (50% < P < 75%) | elevata |
| 5 | molto alta | avviene nella maggior parte dei casi (P > 75%) | catastrofica |

| | 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) |

## 7. Misure che permettono di evitare o mitigare i rischi

### *7.1 Pseudonimizzazione*

All'interno della eCRF vengono utilizzati codici univoci per ciascun paziente/partecipante allo studio. Solo il responsabile della ricerca o altri soggetti autorizzati, possono (con l'uso di mezzi ragionevoli) collegare i codici all'identità dei partecipanti.

### *7.2 Controllo degli accessi logici*

Le credenziali di accesso sono studio specifiche e vengono fornite solo ai PI e al personale autorizzato di AUSL RE IRCCS e dei Centri Partecipanti su richiesta del PI dello studio.

Verrà mantenuto un registro delle utenze attivate che verrà rivisto annualmente. Le utenze non più associate a studi attivi verranno sospese (personale AUSL RE IRCCS) o cancellate (personale esterno). Le utenze del personale esterno all'AUSL RE IRCCS saranno attive limitatamente alla durata prevista dello studio e verranno sospese automaticamente al termine di questo periodo. L'accesso ai progetti sarà automaticamente limitato nel tempo, con la scadenza dei diritti utente impostata sulla data di fine studio indicata nel protocollo o nel modulo di fattibilità locale. Il personale verrà informato in anticipo della sospensione dell'utenza e potrà richiedere l'estensione dell'account, se necessaria e giustificata ai fini dello studio.

L'accesso al database è riservato agli utenti previa autenticazione. Le credenziali degli utenti vengono archiviate in una tabella del database, le password non vengono memorizzate in chiaro, ma prima vengono concatenate con un SALT univoco per ogni utente e poi sottoposte a una funzione crittografica di hashing (SHA-512).

Per aumentare il livello di sicurezza è stata implementata per tutte le utenze, l'autenticazione a 2 fattori, basata sull'utilizzo di codici verifica che saranno inviati alle e-mail istituzionali degli utenti. Tali codici hanno una validità di 2 minuti.
REDCap contiene inoltre un'impostazione di disconnessione automatica, che è personalizzabile (il tempo di disconnessione automatica predefinito è di 30 minuti) e disconnetterà automaticamente un utente dal sistema se non ha svolto alcuna attività (ad esempio facendo clic, digitando, spostando il mouse) sulla pagina web corrente per il periodo di tempo impostato. Ciò impedisce a qualcun altro di accedere all'account e ai dati del progetto se si lascia una stazione di lavoro senza disconnettersi correttamente. Esistono alcune impostazioni personalizzabili che regolano l'attività di accesso, come la possibilità di impostare manualmente il numero di tentativi di accesso non riusciti prima che un utente venga bloccato fuori dal sistema per un periodo di tempo specificato (il numero di tentativi impostato è 5 e il periodo di tempo di attesa è di 15 minuti). È disponibile anche lo stato di sospensione dell'utente, che può essere impostato per qualsiasi utente. La sospensione di un utente consente a un utente di rimanere nel sistema ma nega l'accesso all'intera applicazione REDCap fino a quando il suo stato di sospensione non viene revocato.

Esistono inoltre altre impostazioni di sicurezza specifiche. Queste includono l'impossibilità di riutilizzare le 5 password più recenti e l'obbligo di impostare una nuova password ogni 90 giorni. La password personale deve essere impostata dal singolo utente. L'amministratore di sistema crea il nuovo account e il sistema invia una mail alla persona in oggetto. Nel corpo della mail è specificato lo username assegnato e un link su cui l'utente può cliccare per impostare la propria password. La password deve essere lunga almeno 9 caratteri e contenere lettere minuscole, maiuscole e numeri con durata 90 giorni.
Per garantire che gli utenti REDCap abbiano accesso solo a determinati dati e informazioni, all'interno dell'applicazione vengono utilizzati i privilegi utente. Ogni utente ha il proprio account e il suo account avrà accesso solo ai progetti REDCap a cui il CTC ha concesso l'accesso. I privilegi utente sono inoltre granulari a livello di progetto e possono essere modificati all'interno di qualsiasi progetto dall'amministratore di sistema. All'interno di ogni progetto, sono presenti controlli utente per limitare l'accesso a varie funzionalità e moduli, come la possibilità di esportare dati, inserire dati, aggiungere o modificare campi del database o domande di sondaggi, creare o eseguire report, e così via. È possibile implementare una funzionalità denominata "Data Access Group" per gestire gli studi multicentrici. Questa particolare funzionalità è del tutto facoltativa ma è particolarmente utile in determinate situazioni, come per progetti multi-istituzionali in cui i dati inseriti da un istituto non devono essere accessibili o visualizzabili da altri istituti con accesso allo stesso progetto.
È attivo, inoltre, un sistema di monitoraggio delle vulnerabilità e dei log in tempo reale tramite il software XDR Wazuh.
Le funzionalità più critiche per la sicurezza sono in capo al CTC e agli amministratori di sistema/Data manager:

| **Attività** | **Amministratori di Sistema*** | **Personale del CTC#** |
|---|---|---|
| **Apertura di nuovi progetti sulla piattaforma REDCap** | X | X |
| **Messa in produzione dei progetti** | X | |
| **Creazione di nuove utenze** | X | |
| **Associazione degli utenti ai singoli progetti e profilazione dei privilegi utente per il progetto** | X | X |
| **Archiviazione del progetto** | X | |
| **Accesso a progetti archiviati** | X | |

* Responsabile CTC e Data Manager # Trial Management e Statistica

### *7.3 Partizionamento logico*

Le eCRF sono organizzate secondo partizioni logiche che fanno riferimento allo Studio, il cui accesso è consentito ai singoli Centri Partecipanti arruolanti in forza di sistemi di autorizzazione.
All'interno della eCRF non sono inseriti campi (o combinazioni di campi) che permettano l'identificazione del paziente.

Inoltre, i ruoli degli utenti hanno permessi a diversi livelli: per esempio la funzione di esportazione dati è sotto la responsabilità del Clinical Trial Center. L'esportazione può essere effettuata dal P.I., dal personale dell'area statistica del CTC preventivamente delegato o delegato del P.I in accordo con il protocollo di ricerca.

### *7.4 Crittografia*

I dati sono crittografati sia at rest sia in transit dato che i servizi offerti dagli application server di REDCap sono protetti dalla crittografia dei dati trasmessi mediante protocollo SSL e certificato digitale a 256 bit emesso da Sectigo RSA Organization Validation Secure Server CA; inoltre il protocollo di trasporto dei dati verso l'esterno del sistema è crittografato (SSL / TLS / HTTPS); infine il protocollo di trasporto dei dati tra application server e database è crittografato (SSL / TLS).

### *7.5 Tracciabilità*

REDCap ha un sistema di log interno (audit trail) 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.
In ogni progetto, verranno abilitate di default le funzionalità che permettono di tracciare in modo preciso le modifiche apportate a record già esistenti rendendo obbligatorio fornire un motivo per ogni cambiamento apportato. Questa misura garantisce che ogni modifica sia giustificata e documentata, fornendo un chiaro contesto per le modifiche effettuate. Inoltre promuove la responsabilità tra gli utenti, e offre anche una traccia storica utile per eventuali audit. Verrà inoltre abilitata la cronologia dati e versioni dei file uplodati, mediante cui per ogni dato gli utenti potranno accedere ad un elenco dettagliato delle versioni precedenti, compresi i valori precedenti, l'identità dell'utente che ha effettuato la modifica e il momento in cui è stata apportata, e il motivo per cui è stata eseguita la modifica. I log completi dello studio sono visualizzabili dagli Amministratori di sistema all'interno di uno spazio dedicato.
Questa pagina 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 il periodo di conservazione previsto dal protocollo per la documentazione o comunque in accordo alla normativa applicabile ~~**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).

### *7.6 Archiviazione*

#### 7.6.1 Archiviazione informatica

- il database viene ospitato dal servizio RDS che fornisce un db MySQL.
- Il backup viene effettuato ad ogni modifica effettuata sulla istanza applicativa e giornalmente su RDS con *retention* di 35gg
- 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).

REDCap memorizza i suoi dati e tutte le informazioni di sistema e di progetto in varie tabelle di database relazionali (ovvero utilizzando chiavi e indici esterni) all'interno di un singolo database MySQL, che è un RDBMS (sistema di gestione di database relazionale) open source. Il front-end di REDCap è scritto in PHP, che è un linguaggio di *scripting open source,* robusto e ampiamente utilizzato per le applicazioni web. La configurazione del server web e del server database e la protezione della comunicazione dei server tra loro e con l'utente finale sono responsabilità dell'istituzione partner che sta installando REDCap e pertanto devono essere completate prima dell'installazione di REDCap. L'istituzione che installa REDCap memorizzerà tutti i dati acquisiti in REDCap sui propri server. Pertanto, tutti i dati del progetto vengono archiviati e ospitati presso l'istituzione locale e nessun dato del progetto viene mai trasmesso da REDCap da tale istituzione a un'altra istituzione o organizzazione.
La codifica nativa della pagina Web di REDCap e il confronto di archiviazione del database sono UTF-8, che consente l'utilizzo di lingue non inglesi nel testo definito dall'utente che viene archiviato in REDCap. Ciò include i dati immessi per un progetto o il testo definito per una domanda di sondaggio o un'etichetta di campo del database, oltre a molti altri tipi di testo definiti dall'utente. Le tabelle del database di REDCap implementano il motore di archiviazione Innodb di MySQL, che consente l'uso di chiavi esterne per l'integrità referenziale, le transazioni e il blocco a livello di riga (in contrapposizione al blocco a livello di tabella), tutti necessari in REDCap per coerenza, prestazioni, e scalabilità.

#### 7.6.2 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 alle policy aziendali dell'AUSL RE IRCCS.

### *7.7 Retention dei dati*

I dati verranno raccolti e conservati in accordo con quanto riportato nel protocollo di ricerca o comunque per il tempo previsto dalla normativa applicabile, al termine del quale i dati saranno distrutti in modo sicuro seguendo le linee guida di cancellazione fornite dalle normative di

protezione dei dati e dal massimale di scarto aziendale o completamente anonimizzati in modo tale che non possano più essere attribuiti a un soggetto specifico.

### *7.8 Qualità dei dati*

La qualità dei dati è un aspetto importante della ricerca clinica. Tuttavia durante l'inserimento manuale dei dati esiste la possibilità di commettere errori umani.
Per gestire questa problematica REDCap integra nei moduli di raccolta dati diversi meccanismi che permettono un controllo sui dati inseriti:

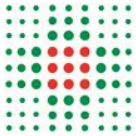
- Validazione dei campi (es. data, testo, numero intero, decimale, ecc)
- Convalida dei dati che limitano i valori che possono essere inseriti (es. date future, minimi e massimi, valori che rispettano logiche predeterminate)
- Gestione dei valori mancanti
- Regole (predefinite e/ o personalizzate) per valutare la qualità e rilevare eventuali discrepanze nei dati raccolti. Dopo aver eseguito la regola all'interno del progetto viene fornito un report sulle discrepanze rilevate in modo da poterle correggere in modo tempestivo.
- "Data Resolution Workflow" (data query). Un sistema attraverso cui è possibile avviare un flusso di lavoro per documentare il processo di risoluzione delle problematiche relative ai dati del progetto (es, aprire, rispondere e chiudere le data queries). Il data Resolution Workflow verrà attivato per gli studi multicentrici in modo da poter garantire un controllo di qualità sui dati inseriti all'esterno dell'AUSL-IRCCS di Reggio Emilia e per favorire e semplificare la risoluzione dei problemi.
- Modulo per il doppio data entry. Questo modulo aggiunge ruoli utente specifici, in modo che gli stessi dati possano essere inseriti indipendentemente da due utenti separati e successivamente verificati da un terzo utente. Il modulo per la gestione del doppio data entry verrà attivato in progetti complessi o di alto profilo e solo se specificato nel protocollo di ricerca.

### *7.9 Controllo degli accessi fisici*

Si considerano gli accessi alle macchine fisiche di AWS.

#### 7.9.1 Accesso ai data center dei dipendenti

AWS offre l'accesso fisico ai data center solo ai dipendenti autorizzati. Tutti i dipendenti che devono accedere al data center devono prima richiedere l'autorizzazione all'accesso e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo. Le richieste vengono vagliate e approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite.



### 7.9.2 Accesso al data center di terzi

L'accesso di terzi deve essere richiesto da dipendenti AWS designati che devono chiedere l'autorizzazione e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo. Tali richieste vengono approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite. Tutti coloro che sono autorizzati all'accesso con il badge visitatore devono presentare al proprio arrivo un documento d'identità, firmare al momento dell'ingresso ed essere scortati dal personale autorizzato.

## *7.10 Protezione da vulnerabilità*

Per aiutare a proteggere i dati archiviati nel database back-end di REDCap, l'applicazione software utilizza vari metodi per proteggersi da utenti malintenzionati che potrebbero tentare di identificare e sfruttare eventuali vulnerabilità della sicurezza nel sistema. Tali metodi verranno descritti qui in dettaglio tecnico. In REDCap, tutti i dati in entrata vengono intenzionalmente filtrati. Ciò include tutti i dati inviati in una richiesta HTTP Post e tutti i dati della stringa di query trovati in ogni URL quando gli utenti accedono a REDCap, oltre alle altre modalità attraverso le quali i dati definiti dall'utente vengono inviati nell'applicazione. Anche le variabili dell'ambiente server vulnerabili alla contraffazione da parte degli utenti finali vengono controllate. Tutti i dati inviati dagli utenti vengono adeguatamente filtrati per eventuali tag potenzialmente dannosi (ad esempio <script>) e vengono quindi sottoposti a escape prima di essere visualizzati su una pagina Web all'interno dell'applicazione. Le query SQL inviate al server database da REDCap vengono tutte correttamente sottoposte a escape prima di essere inviate. Se i valori utilizzati in una query SQL provenissero da valori definiti dall'utente, sarebbero già stati disinfettati in anticipo, come descritto sopra. Per i dati definiti dall'utente utilizzati nelle query SQL viene controllato il tipo di dati per evitare qualsiasi mancata corrispondenza dei tipi di dati (ad esempio assicurandosi che un numero sia realmente un numero). Questi processi di sanificazione, filtraggio, controllo del tipo di dati e fuga aiutano tutti a proteggersi da metodi di attacco, come Cross-Site Scripting (XSS) e SQL Injection. Per proteggersi in modo specifico dal 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" sulle sue pagine Web, in cui esiste un numero massimo stabilito di richieste Web al minuto consentite da un singolo indirizzo IP e, una volta raggiunto tale limite, l'indirizzo IP di quell'utente viene permanentemente bandito da REDCap. Il valore di limitazione della velocità delle richieste al minuto per IP è personalizzabile e può essere modificato nel Contol Center di REDCap, se necessario. La limitazione della velocità previene gli attacchi di tipo Denial of Service da parte dei bot, nonché altri tipi di attacchi hacker che richiedono l'invio di numerose richieste al server in un breve lasso di tempo, come nel caso di un attacco BREACH. Per quanto riguarda specificamente la prevenzione degli attacchi BREACH, oltre a utilizzare la limitazione della velocità, REDCap genera 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. Inoltre, l'uso da parte di REDCap di un token univoco su ogni modulo web riduce notevolmente la possibilità di un attacco BREACH. Molte istituzioni che hanno installato REDCap hanno utilizzato scanner di sicurezza delle applicazioni Web di livello aziendale per scansionare e testare la sicurezza di REDCap e la sua capacità di resistere a vari metodi di attacco. REDCap si è comportato molto bene in questi casi. Qualsiasi istituzione partner che desideri scansionare REDCap utilizzando un software di scansione di sicurezza è libera di farlo senza il consenso della Vanderbilt University o degli sviluppatori di REDCap purché l'istanza particolare di REDCap da scansionare sia la propria e non sia ospitata da un'altra istituzione/organizzazione. Se un'istituzione decide di eseguire una scansione di sicurezza di REDCap e rileva problemi di sicurezza a rischio medio-alto direttamente correlati a REDCap, è incoraggiata a contattare gli sviluppatori di REDCap presso Vanderbilt in modo che tali problemi possano essere risolti immediatamente.
Per quanto riguarda la sicurezza dei cookie utilizzati da REDCap, tutti i cookie di sessione e altri cookie relativi all'autenticazione creati da REDCap avranno automaticamente l'attributo "HttpOnly" impostato su TRUE. Per impostazione predefinita, il flag del cookie "Sicuro" sarà impostato su FALSE. sebbene ciò sia leggermente più insicuro, impostarne il valore su TRUE a volte può causare problemi di accesso con determinate configurazioni del server, come i proxy inversi. Pertanto, per motivi di compatibilità, è impostato come FALSE per impostazione predefinita. Tuttavia, qualsiasi istituzione può abilitare il flag "Sicuro" dei cookie di sessione per migliorare la sicurezza impostando session.cookie_secure=On nel file di configurazione PHP.INI del server web REDCap.
È attivo, inoltre, un sistema di monitoraggio delle vulnerabilità e dei log in tempo reale tramite il software XDR Wazuh.

### *7.11 Monitoraggio continuo delle performance.*

Come già specificato precedentemente è installato sull'istanza applicativa EC2 di REDCap il software XDR open source Wazuh, gestito da Biomeris. Utilizzando Wazuh integrato con OpenCVE e AlienVault, è possibile ottenere una soluzione completa per il monitoraggio delle vulnerabilità e la gestione delle minacce. Wazuh funge da piattaforma centralizzata per il rilevamento delle anomalie e la risposta agli incidenti, raccogliendo log e analizzando gli eventi in tempo reale. L'integrazione con OpenCVE consente a Wazuh di ricevere aggiornamenti sulle vulnerabilità pubblicamente note (CVE), migliorando l'efficacia del monitoraggio di sicurezza. AlienVault, inoltre, arricchisce i dati con informazioni sulle minacce provenienti da fonti globali, offrendo un contesto più ampio e dettagliato per ogni evento. BIOMERIS ha inoltre aggiunto una serie di controlli personalizzati volti a identificare comportamenti anomali (e.g. elevato uso di CPU, elevato traffico dati). Questo approccio integrato garantisce che le performance siano costantemente monitorate e protette, riducendo i rischi e permettendo interventi rapidi in caso di criticità.

### *7.12 Lotta contro il malware*

È stato installato all'interno dell'istanza applicativa il sistema antivirus open source ClamAV che garantisce una efficace protezione da malware e virus

### *7.13 Backup e ripristino*

L'istanza applicativa di REDCap è ospitata su Amazon EC2, e viene eseguito un backup manuale (AMI) dell'istanza prima e dopo ogni attività di manutenzione del software REDCap e delle componenti necessarie al suo funzionamento. Le AMI (Amazon Machine Images) generate dalla console EC2 sono salvate automaticamente in S3 (Simple Storage Service), anche se non sono direttamente visibili o accessibili tramite S3. AWS utilizza S3 come infrastruttura di supporto per memorizzare in modo sicuro le AMI, garantendo durabilità e affidabilità dei backup. Per il database, ospitato su Amazon RDS, è configurato un backup automatico eseguito ogni notte. I backup vengono conservati per 35 giorni, e la configurazione consente un ripristino in una data specifica all'interno di questo periodo. Il ripristino del database su Amazon RDS è possibile attraverso la console di AWS e può essere completato in modo rapido, minimizzando i tempi di inattività.

### *7.14 Aggiornamento*

REDCap è una piattaforma in costante sviluppo e miglioramento, con nuove versioni rilasciate regolarmente per potenziare funzionalità e sicurezza.
L'istanza REDCap in uso è aggiornata annualmente all'ultima versione LTS (Long Term Support) disponibile. La versione LTS rappresenta una release stabile e supportata a lungo termine, che garantisce maggiore affidabilità e continuità operativa.
Ogni settimana, l'amministratore di sistema verifica, sulla pagina ufficiale dello sviluppatore, il rilascio di nuove versioni e le modifiche implementate; qualora vengano introdotte correzioni che riguardano funzionalità di sicurezza ritenute rilevanti, anche se non classificate come critiche, si valuterà insieme al team di BIOMERIS la necessità di un aggiornamento non programmato. BIOMERIS SRL si fa carico delle attività di manutenzione ordinaria e degli aggiornamenti dell'applicativo.

### *7.15 Sviluppo sicuro*

Lo sviluppo delle integrazioni è basato sulle API di REDCap. Lo sviluppo delle procedure di integrazione da e verso la piattaforma REDCap viene effettuato seguendo le linee guida interne di BIOMERIS. Le linee guida prevedono lo sviluppo in un ambiente di test, una fase di verifica e una di validazione prima di portare il processo in produzione. Inoltre, è importante menzionare l'utilizzo all'interno dell'IDE di sviluppo dell'estensione SonarLint che permette di migliorare la qualità del codice e di individuare potenziali problemi e vulnerabilità in fase di scrittura.

### *7.16 Protezione contro fonti di rischio non umane*

Le garanzie di Amazon AWS sui server sono molteplici, tra cui le seguenti
*Alimentazione*
I sistemi di energia elettrica che alimentano i nostri data center sono completamente ridondanti e la loro manutenzione può essere eseguita senza alcun impatto sull'operatività, 24 ore al giorno. AWS

garantisce che i propri data center sono dotati di generatori di back-up per non interrompere le operazioni di carichi strategici e critici in caso di interruzione dell'energia elettrica presso la struttura.

*Clima e temperatura*

I data center AWS utilizzano meccanismi di controllo del clima e della temperatura per garantire le condizioni ottimali per server e altro hardware, evitare eventuali surriscaldamenti e ridurre al minimo possibili disservizi. Il personale e i sistemi monitorano e verificano che umidità e temperatura rimangano entro i limiti stabiliti.

*Rilevamento ed estinzione del fuoco*

I data center AWS sono dotati di attrezzature automatiche per il rilevamento e l'estinzione delle fiamme. Tali sistemi utilizzano sensori di rilevamento del fumo all'interno di spazi dedicati alla rete, alle infrastrutture e a componenti meccanici. Tali aree sono anche protette da sistemi di estinzione delle fiamme.

*Rilevamento di perdite acqua*

Per individuare la presenza di perdite, AWS installa presso i propri data center sistemi in grado di rilevare la comparsa di acqua. In questo caso, si attivano meccanismi in grado di rimuovere l'acqua per evitare eventuali danni aggiuntivi.

### *7.17 Contratto con il responsabile del trattamento*

Tutti i soggetti terzi che prestano servizi necessari per la conduzione dello Studio vengono nominati Responsabili del trattamento, mediante contratto sottoscritto ai sensi dell'art. 28 del GDPR.

### *7.18 Revisione DPIA*

È prevista una revisione annuale del Data Protection Impact Assessment (DPIA) come parte di un processo sistematico per garantire una valutazione continua dei rischi legati al trattamento dei dati personali in relazione all'utilizzo della piattaforma REDCap. Questo approccio consente di identificare eventuali vulnerabilità e di adottare le misure necessarie per garantire la conformità alle normative sulla protezione dei dati. In tale processo sono coinvolti gli amministratori di sistema, il DPO, il responsabile privacy aziendale, il responsabile del trattamento dei dati e lo STIT per garantire che REDCap sia conforme alle normative vigenti sulla protezione dei dati e soddisfi i requisiti tecnici, organizzativi e di sicurezza necessari.

### *7.19 Revisione dei processi per la conformità GDPR e normativa vigente*

Gli amministratori di sistema si manterranno costantemente aggiornati sulle normative in materia di privacy e trattamento dei dati personali e sensibili trattati con finalità di ricerca, anche mediante la partecipazione ad attività formative sul tema interne ed esterne all'Azienda. Le misure di carattere organizzativo saranno riviste periodicamente, consentendo così di identificare e correggere tempestivamente eventuali discrepanze e garantendo la conformità alle normative vigenti. In questo processo saranno consultati il DPO e il responsabile privacy aziendale.

### *7.20 Gestione del personale*

AUSL RE IRCCS eroga formazione periodica agli operatori su:

- Utilizzo della piattaforma REDCap
- Inserimento dei dati nelle eCRF
- Normativa relativa agli studi clinici e in materia di dati personali.
- Data management
- Pishing (formazione aziendale)

Sono state implementate misure di carattere organizzativo per la gestione degli accessi, la creazione delle eCRF/survey e la verifica delle stesse prima della messa in produzione dello studio clinico. Tutti i progetti saranno sottoposti ad un controllo preventivo alla messa in produzione da parte dell'amministratore di sistema/Data manager. Questo controllo riguarderà sia la struttura e l'appropriatezza delle eCRF, l'aderenza al protocollo e il rispetto delle normative in materia di privacy e protezione dei dati. Requisito fondamentale per la messa in produzione è il nullaosta (se applicabile). È in corso la stesura di procedure operative scritte specifiche.

## 8. Conformità al GDPR e alle normative sulla protezione dei dati

### *8.1 Base giuridica per il trattamento*

Il trattamento dei dati avverrà sulla base del consenso al trattamento dei dati dei partecipanti allo studio clinico/progetto di ricerca/survey, approvato, se applicabile, dal Comitato Etico competente e i dati raccolti saranno utilizzati esclusivamente per le finalità dichiarate.
Nel caso di studi retrospettivi su soggetti per i quali non sia possibile acquisire il consenso, sarà possibile utilizzare i dati anche senza consenso esplicito nei casi e con le modalità previste dagli artt. 110 e 110 bis, comma 4, del Codice Privacy e dei Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali (Provvedimento n. 298 del 9/5/2024 e FAQ del 6/5/2024).

### *8.2 Diritti degli interessati*

I soggetti arruolati potranno esercitare i loro diritti di accesso, rettifica, cancellazione, limitazione dei dati.
Il Principal Investigator e l'équipe che ha in carico il paziente/soggetto fornisce adeguata informativa e nei casi previsti acquisisce il consenso al trattamento.

## 9. Consultazione del DPO e degli stakeholder

### *9.1 Consultazione del DPO*

Il DPO è stato consultato durante la fase di pianificazione e implementazione del sistema REDCap.

### *9.2 Consultazione con gli stakeholder*

Sono stati coinvolti gli amministratori di sistema, il responsabile privacy aziendale, il responsabile del trattamento dei dati e lo STIT per garantire che REDCap soddisfi i requisiti tecnici, organizzativi e di sicurezza necessari per il progetto.

## 10. Conclusione della DPIA

### *10.1 Esito della DPIA*

I rischi identificati sono stati mitigati con misure di sicurezza robuste e conformi al GDPR. A seguito dell'implementazione delle misure di sicurezza il livello di rischio residuo è considerato accettabile. Pertanto il progetto può procedere con l'implementazione e l'uso di REDCap per la raccolta e gestione dei dati clinici in modo sicuro.

### *10.2 Piano di monitoraggio*

Verranno eseguiti audit regolari per garantire che le misure di sicurezza siano adeguate e che i rischi siano continuamente monitorati e gestiti.

## 11. Firma e approvazione

Parere favorevole DPO
Erica Molinari

Erica
Molinari
19.05.2025
15:31:36
GMT+02:00

Per il Titolare del trattamento
Il Direttore Generale
Davide Fornaciari

**LA PRESENTE COPIA E' CONFORME ALL'ORIGINALE DEPOSITATO.**
**Elenco firme associate al file con impronta SHA256 (hex):**
**CEE1D18FC145358B57BFB2DDE94D147874ECDCB7060DE3766156B2233694CD82**

Firma di Davide Fornaciari. Data firma: 22/05/2025
Firma di Erica Molinari. Data firma: 19/05/2025