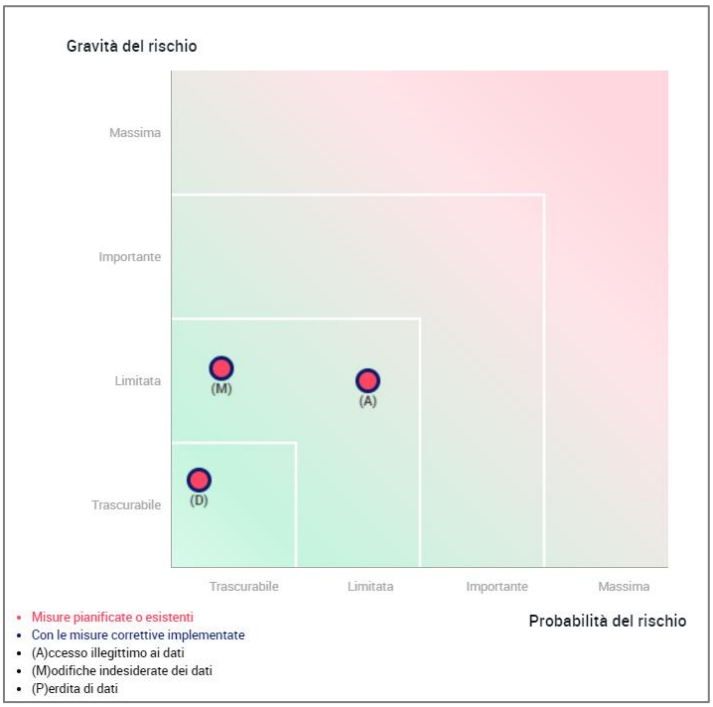
DPIA Studi osservazionali GIMEMA (con pazienti non ricontattabili e trasferimento dati extra-UE)

Editing : Fondazione GIMEMA Franco Mandelli Onlus
Evaluation : Maria Valeria Feraco, Luca Pizzato
Validation : Rosalba Cucci
Status :Validata 100%

Mappaggio dei rischi



DPO and data subjects opinion

Nome del DPO/RPD

Marco Ferrante

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Il trattamento può essere implementato in quanto la base giuridica risulta correttamente individuata e il Titolare ha implementato misure tecnico-organizzative adeguate.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Nel caso di specie non sussistono le condizioni per richiedere il parere degli interessati atteso che la Fondazione opera in veste di Promotore di studio clinico e non ha accesso diretto all'identità ed ai contatti dei pazienti.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Gestione dei dati dei pazienti arruolati nell'ambito degli studi osservazionali retrospettivi e prospettici promossi da GIMEMA.

Quali sono le responsabilità connesse al trattamento?

Titolari autonomi del trattamento: Fondazione GIMEMA Franco Mandelli Onlus e Centro Sperimentatore (conforme all'approccio indicato dalle Linee guida del Garante italiano per la protezione dei dati personali del 24 luglio 2008).
Seeweb srl nominato responsabile del trattamento ex art. 28 GDPRcon funzione di cloud provider.
Dott. Luca Pizzato e dott. Giulio Pandolfelli nominati ADS del sistema di raccolta dati REDCap.

Ci sono standard applicabili al trattamento?

Non esistono veri e propri standard, tuttavia ci si conforma alle Linee Guida per i trattamenti dei dati personali nell'ambito delle sperimentazioni cliniche di medicinali del 24 luglio 2008, nonchè alle pertinenti prescrizioni contenute nelle Autorizzazioni generali nn. 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il dlgs. n. 101/2018 di adeguamento del Codice come individuate dal Provvedimento del Garante n. 497 del 13 dicembre 2018, per quanto applicabile al Parere 5/2014 sulle tecniche di anonimizzazione del WP art.29.

Valutazione : Accettabile
Commento di valutazione :
Ruoli e responsabilità del trattamento sono puntualmente definiti.

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Nell'ambito degli studi in oggetto sono trattati i seguenti dati dei pazienti:
A) Dati anagrafici
B) Dati genetici e relativi allo stato di salute

I dati oggetto di questo trattamento sono pseudonimizzati e soltanto lo sperimentatore del Centro ha la facoltà di risalire tramite lista all'identità del paziente (confome all'approccio indicato dalle Linee guida del Garante per la protezione dei dati personali del 24 luglio 2008).

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I dati saranno raccolti nel corso degli studi in oggetto all'interno delle CRF elettroniche, disegnate appositamente per ciascuno studio all'interno del sistema informatico REDCap.

I dati saranno registrati, elaborati e conservati unitamente ad un codice che identificherà il paziente. La gestione dei dati avrà oggetto le attività di inserimento, verifica, correzione e aggiornamento proprie dell'attività di data management all'interno degli studi in oggetto (conformemente alle indicazioni contenute nelle Linee guida del Garante italiano per la protezione dei dati personali del 24 luglio 2008).

Terminata la raccolta e la verifica dei dati, si procede con l'analisi statistica dei dati pseudonimizzati, come descritto nel protocollo scientifico di ogni studio.

I dati degli studi in oggetto saranno conservati per un tempo corrispondente a 25 anni, conformemente alle disposizioni di legge.

Possono accedere ai dati pseudonimizzati di tutti i pazienti degli studi in oggetto i dipendenti della Fondazione che svolgono attività di data management nell'ambito degli studi in oggetto, appositamente autorizzati al trattamento nel rispetto del principio del "*need to know*" e specificatamente formati sulle tematiche del GDPR, con riferimento al trattamento dei dati per finalità di ricerca scientifica.

I dati degli studi in oggetto non saranno diffusi. Le pubblicazioni dei risultati avverranno nelle modalità previste dal protocollo scientifico e dalla normativa regolatoria di settore e comunque in forma rigorosamente anonima. Il processo di anonimizzazione avviene in modalità conformi agli standard di cui all'Opinion 05/2014 *on Anonymisation Techniques* del Working Party art.29.

La partecipazione del paziente agli studi in oggetto implica che, in conformità alla normativa sulle sperimentazioni cliniche dei medicinali, il personale del Comitato Etico e le autorità sanitarie italiane potranno conoscere i dati degli studi, senza poter risalire all'identità del paziente.

Quali sono le risorse di supporto ai dati?

I soggetti coinvolti sono:
- Dott. Luca Pizzato e Giulio Pandolfelli come ADS.
- Tecnici di Seeweb srl incaricati come ADS da Seeweb, (società che, come sopra precisato, è nominata responsabile del trattamento), per operazioni di manutenzione e supporto tecnico.
- Personale GIMEMA incaricato come data manager degli studi in oggetto.

L'unico documento cartaceo contenente dati personali è il consenso informato dello studio, ove previsto, che unitamente all'informativa sul trattamento dei dati personali viene somministrato al paziente dallo sperimentatore del Centro che lo ha in cura e conservato presso lo stesso.

I dati originali sono annotati nelle cartelle cliniche conservate presso il Centro sperimentatore. GIMEMA, quale promotore, non ha accesso alle cartelle cliniche dei pazienti.

Valutazione : Accettabile
Commento di valutazione :

Il trattamento è svolto in accordo alle Linee Guida per i trattamenti dei dati personali nell'ambito delle sperimentazioni cliniche - 24 luglio 2008, nonché alle pertinenti prescrizioni contenute nelle Autorizzazioni generali nn. 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice come individuate dal Provvedimento del Garante n. 497 del 13 dicembre 2018.

Il ciclo di vita del trattamento e le risorse di supporto ai dati sono analiticamente descritte.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La finalità del trattamento per gli studi osservazionali in oggetto è esplicitata all'interno dell'informativa privacy somministrata al paziente per ciascuno studio.

Valutazione : Accettabile
Commento di valutazione :
Si, come esplicitato nell'informativa studio specifica.

Quali sono le basi legali che rendono lecito il trattamento?

Il consenso del paziente per i pazienti ricontattabili, in difetto per i pazienti deceduti e/o non ricontattabili troverà applicazione l'Art. 110 d.lgs 196/03.

Valutazione : Accettabile
Commento di valutazione :

La base giuridica è coerente con la normativa applicabile, con le specifiche indicazioni del garante contenute nelle citate Linee guida e Prescrizoni, ed è riportata nell'informativa resa ai pazienti al momento dell'arruolamento, nonché preliminarmente vagliata dal Comitato Etico competente.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Si, sono raccolti solo quei dati necessari a determinare i risultati degli studi in oggetto, ovvero secondo gli obiettivi progettati prima dell'arruolamento dei pazienti e descritti puntualmente all'interno del protocollo scientifico dello specifico studio.

Valutazione : Accettabile
Commento di valutazione :

Si, sono raccolti solo quei dati necessari a determinare i risultati degli studi in oggetto, ovvero secondo gli obiettivi progettati prima dell'arruolamento dei pazienti e descritti puntualmente all'interno del protocollo scientifico dello specifico studio.

I dati sono esatti e aggiornati?

Si, vengono adottate misure di correzione e aggiornamento dei dati, automatiche e manuali, previste dall'attività di data management dello studio. Tale attività comporta l'esecuzione e la risoluzione di queries all'interno delle CRF elettroniche. Il sistema prevede un meccanismo di controllo, audit trail, che permette per i dati inseriti nel sistema la tracciabilità a ritroso al dato originale documentando ogni alterazione di questo.

Valutazione : Accettabile
Commento di valutazione :

Si, è previsto un meccanismo di controllo dei dati di ciascun studio, inseriti nella piattaforma REDCap.

Qual è il periodo di conservazione dei dati?

I dati degli studi in oggetto saranno conservati per un tempo corrispondente a 25 anni, conformemente alle disposizioni di legge.

Valutazione : Accettabile
Commento di valutazione :

La valutazione da migliorabile si definisce oggi accettabile poichè la Fondazione GIMEMA ha realizzato il piano d'azione programmato nel 2019 come proposta di miglioramento, in relazione al periodo di conservazione dei dati relativi agli studi promossi dalla Fondazione.

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Agli interessati viene resa informativa ex art.13 GDPR da parte del Centro sperimentatore secondo il modello predisposto da GIMEMA per gli studi in oggetto e preliminarmente approvato dal competente Comitato Etico.

Valutazione : Accettabile
Commento di valutazione :

L'informativa contiene tutti gli elementi previsti dall'art.13 del GDPR.

Ove applicabile: come si ottiene il consenso degli interessati?

Lo sperimentatore del Centro, che ha in cura il paziente, prima di procedere all'arruolamento nello studio, fornisce l'informativa privacy, esplicitandone i contenuti e raccogliendo il relativo consenso/i in forma scritta attraverso la dichiarazione in calce all'informativa.

Valutazione : Accettabile
Commento di valutazione :

Il consenso viene acquisito direttamente dagli interessati in via preventiva rispetto al trattamento.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Nell'informativa vengono forniti i contatti di entrambi i titolari del trattamento (GIMEMA e Centro sperimentatore) e le indicazioni in merito alle modalità di esercizio dei diritti. Il relativo riscontro da parte della Fondazione è assicurato e disciplinato da apposita procedura per la "gestione dei diritti degli interessati".

Valutazione : Accettabile
Commento di valutazione :

L'informativa indica la procedura per l'esercizio degli indicati diritti.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Nell'informativa vengono forniti i contatti di entrambi i titolari del trattamento (GIMEMA e Centro sperimentatore) e le indicazioni in merito alle modalità di esercizio dei diritti. Il relativo riscontro da

parte della Fondazione è assicurato e disciplinato da apposita procedura per la "gestione dei diritti degli interessati".

Valutazione : Accettabile
Commento di valutazione :

L'informativa indica la procedura per l'esercizio degli indicati diritti.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Nell'informativa vengono forniti i contatti di entrambi i titolari del trattamento (GIMEMA e Centro sperimentatore) e le indicazioni in merito alle modalità di esercizio dei diritti. Il relativo riscontro da parte della Fondazione è assicurato e disciplinato da apposita procedura per la "gestione dei diritti degli interessati".

Valutazione : Accettabile
Commento di valutazione :

L'informativa indica la procedura per l'esercizio degli indicati diritti.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Si, sono disciplinati dai contratti e dagli atti di nomina a responsabili del trattamento, redatti nel rispetto dei requisiti di cui all'art. 28 GDPR.

Valutazione : Accettabile
Commento di valutazione :

Si, sono disciplinati in apposito atto di nomina.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati vengono trasferiti extra-UE solo per finalità di farmacovigilanza, per la segnalazione degli eventi avversi all'azienda coinvolta nello specifico studio.

Le segnalazioni, che possono contenere dati in forma pseudonimizzata (e.g. patient ID, genere e età), sono gestite dall'Azienda in compliance con il GDPR.

Sul punto si osserva che:

a) ai sensi dell'art. 5 comma 2 DM Salute 30.11.2021 recante Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52, "**Le imprese farmaceutiche aventi titolo sul medicinale oggetto di sperimentazione e i promotori delle sperimentazioni senza scopo di lucro hanno il reciproco obbligo di comunicarsi i dati di sicurezza per i successivi adempimenti in materia di farmacovigilanza** e sicurezza delle sperimentazioni cliniche e per le decisioni di propria competenza".

b) a mente dell'art. 49 del GDPR, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (tra l'altro) allorquando il trasferimento sia necessario per importanti motivi di interesse pubblico riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

c) l'attività di farmacovigilanza rientra nel novero delle attività di rilevante interesse pubblico ai sensi dell'art. 2 sexies comma 2, lett. z) d.lgs. 196/03 come novellato dal d.lgs. 101/2018.

Il trasferimento avviene pertanto per motivi di interesse pubblico rilevante ai sensi dell'art. 49 comma 1lett. d GDPR.

Valutazione : Accettabile
Commento di valutazione :
La valutazione è accettabile perchè conforme a quanto previsto dal capo V del GDPR.

Rischi

Misure esistenti o pianificate

Controllo degli accessi logici

Una volta completate le pratiche regolatorie ed ottenuto il parere favorevole del Comitato Etico, il Centro sperimentatore può essere aperto all'arruolamento dei pazienti. Il Centro compila una form in cui occorre indicare i soggetti autorizzati alla compilazione delle e-CRF. Ricevuto il form, l'assistenza tecnica GIMEMA crea gli account per il Centro.

L'accesso è permesso ai soli autorizzati al trattamento tramite username e password assegnate personalmente. Agli account sono applicati criteri di sicurezza per ridurre il rischio illegittimo o comunque non qualificato quali:

- Profilazione degli utenti, autorizzati al trattamento, secondo le responsabilità attribuite da GIMEMA.

- Password e unersame univoci e personali, composte da almeno 8 caratteri (comprendente di maiuscolo, minuscole, numeri e caratteri speciali), costituenti le credenziali di autenticazione dell'incaricato.

- Dopo l'inserimento delle credenziali per accedere alla piattaforma è necessaria una seconda autenticazione tramite uno dei servizi seguenti a scelta dell'utente: google authenticator, microsoft authenticator, sms (twillio) e e-mail.

- Cambiamento obbligatorio delle password ogni 90 giorni. All'utente verrà richiesta la creazione di una nuova password alla scadenza.

- I codici identificativi personali sono disattivati in caso di non utilizzo per più di 6 mesi.

- Dopo 3 tentativi di login l'utente della piattaforma è bloccato per 600 minuti.

- Dopo un periodo di inattività di 30 minuti viene effettuato un logoff automatico che richiede un nuovo login.

L'accesso come amministratore del server (root) avviene secondo le seguenti modalità:
- Connessione tramite VPN per accedere alla rete privata.
- Accesso al server con chiave privata (SHA-256) in possesso esclusivo dell'ADS.
- Accessi non corretti vengono bloccati dopo massimo 2 tentativi tramite il servizio fail2ban.

L'accesso come amministratore ai server è monitorato tramite il sistema WAZUH, che invia una e-mail alla Fondazione per ogni accesso riuscito o non riuscito ai server. Tale e-mail non è sotto il controllo degli amministratori di sistema. Settimanalmente alla stessa e-mail viene inviato un report degli accessi.

Valutazione : Accettabile
Commento di valutazione :

Le misure sono congrue.

Minimizzazione dei dati

La raccolta dei dati dei pazienti arruolati da parte del promotore avviene esclusivamente in mjodalità pseudonimizzata attraverso il relativo inserimento nelle CRF.
Fermo il filtro iniziale alla raccolta stessa dei dati, che non consente la raccolta di dati ulteriori rispetto a quelli indicati nel protocollo come strettamente necessari alla conduzione dello studio, lo stesso accesso agli stessi è rigorosamente limitato nel seguente modo:

- il Centro sperimentatore può accedere solo ai dati dei pazienti da lui registrati. Gli accessi sono

forniti da GIMEMA e protetti da password criptata;
- gli ADS incaricati da GIMEMA hanno accesso a tutti i dati registrati nel sistema solo quando strettamente necessario (manutenzione, assistenza tecnica e aggiornamento del sistema);
- i dipendenti GIMEMA con ruolo di data manager per lo studio specifico hanno accesso a tutti i dati dello studio.

I dati sono registrati e conservati nel database di ciascuno studio unitamente ad un codice, univoco per ciascun paziente. I dati sono, pertanto, pseudonimizzati e solo lo sperimentatore del Centro ha facoltà di risalire al nominativo del paziente.

Valutazione : Accettabile
Commento di valutazione :

Le misure sono congrue.

Politica di tutela della privacy

GIMEMA ha nominato un DPO nella figura dell'Avv. Marco Ferrante ed ha adottato specifiche policy e procedure per assicurare a corretta gestione dei dati personali.

Valutazione : Accettabile
Commento di valutazione :

Il DPO vigila sul costante rispetto del GDPR e di tutta la normativa in materia di trattamento dei dati personali da parte della Fondazione.

Gestione postazioni

Ogni utente autorizzato è responsabile della gestione della sicurezza limitatamente alle postazioni che utilizzano per accedere al sistema, così come della conservazione della propria password.

I server WEB E DB sono protetti da VPN distinte per l'infrastruttura di produzione e di disaster recovery.

Per accedere è necessario autenticarsi alla VPN con credenziali personali e un certificato personale rilasciato dalla VPN stessa. Successivamente è possibile autenticarsi al server con credenziali personali. Le coppie user/password, end point di accesso e certificati sono gestiti personalmente dall'ADS e salvati in un gestionale di password sicuro. Nessuna di queste informazioni sono salvate, anche temporaneamente, sui dispositivi personali. Accesso a queste informazioni sono rese disponibili anche al Responsabile del Centro Dati per politiche di continuità operativa.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Tracciabilità

l sistema prevede il tracciamento di tutte le attività dell'utente registrato (accessi, pagine visualizzate, dati inseriti/modificati, ecc.) e la possibilità di visualizzare i dati in forma tabellare o grafica da parte degli amministratori di sistema e dei responsabili di progetto.

Sono anche registrati tutti gli avvisi automatici inviati agli utenti per il corretto funzionamento del database.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Vulnerabilità

L'infrastruttura è collegata al un sistema SIEM (Security Information and Event Management) basato su Wazuh.
La soluzione raccoglie e analizza in tempo reale i log di sistema, gli accessi utente, le metriche di performance e gli eventi di sicurezza dei server in ambiente LAMP. Il sistema monitora l'integrità dei file, rileva potenziali minacce e vulnerabilità, e genera alert automatici per eventi critici. Per i database MySQL vengono monitorate metriche specifiche come connessioni, performance delle query e stato della replicazione. Tutti i dati vengono centralizzati su un manager dedicato che applica regole di correlazione per identificare anomalie e incidenti di sicurezza.
Reportistica riguardo lo stato dell'infrastruttura (aggiornamenti necessari, audit trail, ecc.) è esportabile in ogni momento dal sistema di monitoring.

Valutazione : Accettabile
Commento di valutazione :
La valutazione da migliorabile si definisce oggi accettabile in relazione alle nuove misure implementate.

Pseudonimizzazione

I dati sono registrati e conservati nel database di ciascuno studio unitamente ad un codice, univoco per ciascun paziente. I dati sono, pertanto, pseudonimizzati e soltanto lo sperimentatore del Centro ha la facoltà di risalire al nominativo del paziente.

La pseudonimizzazione è garantita nel rispetto delle linee guida *Guidelines 01/2025 on Pseudonymisation of European Data Protection Board.*

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Lotta contro il malware

Gli amministratori di sistema (ADS) utilizzano un gestore password professionale (1Password) per salvare e gestire in modo sicuro tutte le password e le chiavi di accesso ai server. Questo approccio garantisce:

- Memorizzazione criptata delle credenziali
- Generazione di password complesse e uniche per ogni servizio
- Condivisione sicura delle credenziali tra gli amministratori autorizzati
- Tracciamento degli accessi alle credenziali
- Riduzione del rischio di riutilizzo delle password

Tutti gli accessi ai server sono protetti mediante una soluzione VPN basata su OPNsense con le seguenti caratteristiche:

- Accesso esclusivo agli amministratori di sistema (ADS)
- Autenticazione a più fattori per la connessione VPN
- Isolamento della rete di gestione dei server
- Firewall che permette pubblicamente solo la connessione all'applicativo. Tutte le porte di servizio sono filtrate dalla VPN stessa.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Sicurezza dei siti web

La connessione remota alla piattaforma REDCap avviene tramite certificato SSL rilasciato da RapidSSL. Il download di documenti (es. documenti PDF) dalla piattaforma avviene tramite lo stesso certificato di sicurezza o utilizzando il sistema interno di invio file che invia una mail usando la cifratura TLS.

I cookie registrati dalla piattaforma sono cookie tecnici per permettere il nomale funzionamento del sistema di raccolta dati.
Per ridurre il rischio di intrusioni nel sistema, dall'esterno l'architettura informatica prevede due server (WebServer e DB Server) protetti da VPN privata. Tale VPN permette solo l'accesso pubblico tramite protocollo https. Tutte le altre porte sono bloccate all'accesso pubblico.

Il DB server non è accessibile direttamente da web se non con accesso VPN e chiave privata in possesso dell'ADS.
Sono effettuati controlli periodici sui log di sistema per analizzare eventuali tentativi di accesso non autorizzato.

Viene eseguita ad intervalli temporali regolari una security checklist, che include test di accessi non autorizzati, analisi dei log di sistema, test dell'efficacia del firewall e altre misure al fine di testate, verificare e valutare l'efficacia delle misure di sicurezza analogiche adottate in ambito software.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Backup

Dal punto di vista tecnico le impostazioni di default del servizio prevedono il backup incrementale di tutto il file system, nello specifico la procedura di backup prevede un primo processo di archiviazione su nastro di tutti i dati fisici (file e cartelle) presenti sul Cloud Server. In seguito alla prima esecuzione del backup verrà eseguito periodicamente, in base alla tipologia di prodotto acquistato copiando solamente i file modificati dall'ultima esecuzione. La copia dei dati resterà a disposizione sul sistema di backup fino in quando non verrà eliminata dal disco. Da quel momento la copia presente sul backup verrà impostata in uno stato "inattivo" e potrà essere recuperata entro i successivi 30 giorni. Nel caso in cui il file venga sovrascritto piuttosto che cancellato la successiva esecuzione del backup imposterà la copia precedente nello stato "inattivo" e quella attuale nello stato "attivo". La copia "inattiva" verrà cancellata solo dopo 30 giorni oppure nel caso in cui il dato venga modificato nuovamente.

Con il backup giornaliero o settimanale vengono mantenute in memoria di backup una copia attiva ed una copia inattiva dello stesso file, con il backup giornaliero o settimanale 7 versioni verrà conservata una copia attiva e sei copie inattive.

Il CDMA REDCap opera utilizzando quattro Cloud Server così configurati:

Nome Server	Destinazione Backup	Periodo di mantenimento dati	Tempi di backup
Web Server Produzione	Tivoli Storage	30 giorni	Una volta a settimana
DB Server Produzione	Tivoli Storage	30 giorni	Ogni giorno
Web Server DR	Tivoli Storage	30 giorni	Una volta a settimana
DB Server DR	Tivoli Storage	30 giorni	Una volta a settimana

I tempi di ripristino dei backup sono i seguenti:

Recovery Point Objective (RPO): 24 Ore
Indica la quantità massima di dati che può essere persa in caso di interruzione o disastro. Si misura in tempo e rappresenta il punto temporale fino al quale i dati devono essere recuperabili.

Recovery Time Objective (RTO): 24 Ore
Definisce il tempo massimo entro il quale un sistema, un'applicazione o un processo aziendale devono essere ripristinati dopo un'interruzione, per ridurre l'impatto sull'operatività.

DISASTER RECOVERY
Il sistema di disaster recovery implementato prevede una macchina virtuale con caratteristiche identiche all'originale, in cui vengono sincronizzati tutti i dati in modalità real time. In caso di failure il traffico viene indirizzato verso l'infrastruttura di replica verificando con il cloud provider l'effettivo funzionamento del sistema. Alla risoluzione dell'eventuale problema dell'infrastruttura di produzione i sistemi vengono sincronizzati per ripristinare il sistema di produzione.
I tempi di ripristino del DR sono i seguenti:
Recovery Point Objective (RPO): 8 ore
Recovery Time Objective (RTO): 8 ore

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Manutenzione

Vedere documento di sicurezza Seeweb allegato.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Sicurezza dell'hardware

I server web e database sono ospitati da Seeweb srl.

Tutti gli impianti sono dotati delle più moderne tecnologie di sicurezza, relativamente agli accessi, alla sorveglianza, alle intrusioni, alla prevenzione e all'estinzione degli incendi.

Gli impianti sono dotati di refrigerazione ridondata, di alimentazione protetta sia da gruppi statici sia da gruppi elettrogeni diesel a lunga autonomia e ridondanti.

Seeweb dispone della certificazione di processo ISO9001, di compatibilità ambientale ISO14001 e di sicurezza nel trattamento dei dati ISO27001. Per ulteriori dettagli vedere documento sicurezza Seeweb allegato.

Le certificazioni SeeWeb sono presenti nel loro sito https://www.seeweb.it/azienda/certificazioni e sono disponibili per la consultazione pubblica.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Crittografia

L’accesso alla piattaforma on-line è protetto da cifratura tramite SSL

- la piattaforma è accessibile solo con protocollo di trasmissione dati HTTPS (con cifratura dei dati);
- viene utilizzato Secure Socket Layer 256-bit encryption con protocollo TLS 1.3;
- certificato Digicert.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Archiviazione

Alla chiusura in toto di ogni studio il database viene archiviato sulla piattaforma REDCap. L'accesso è consentito esclusivamente agli amministratori di sistema e tutte le altre autorizzazioni alla lettura sono rimosse (Centri, Data Manager).

Una copia dell'intero database di ogni studio è conservata in una cartella in sola lettura su uno spazio cloud (Seeweb srl) a disposizione dell'area statistica. L'accesso a tale area è limitato solo agli utenti autorizzati e protetto da rete privata VPN.

Gli unici ad avere permessi di scrittura nella cartella sono gli ADS.

Le misure di sicurezza relative al sistema sono disponibili nel documento di sicurezza di Seeweb, nominato come responsabile del trattamento.

Valutazione : Accettabile
Commento di valutazione :

La valutazione da migliorabile si definisce oggi accettabile.
Al fine di migliorare la procedura di archiviazione, l'Area IT con gli ADS hanno implementato a partire dal mese di febbraio 2023 un ambiente dedicato in sola lettura in cui archiviare una copia del database al momento della chiusura dello studio.

Gestione delle politiche di tutela della privacy

E' prevista una revisione annuale delle politiche e procedure di tutela della privacy.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Contratto con il responsabile del trattamento

Seeweb srl nominato Responsabile del trattamento dei dati con funzione di cloud provider (vedere nomina allegata).

Dr Luca Pizzato e dr Giulio Pandolfelli nominati ADS del sistema di raccolta dati, ovvero la piattaforma REDCap (vedere nomina allegate).

IWG nominato Responsabile del trattamento dei dati personali in riferimento al sistema gestionale Sharepoint (vedere nomina allegata).

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Quando si verificano non conformità, successivamente ad una valutazione dell'impatto eventuale sulla qualità del servizio, si definisce se devono essere condotte indagini di ROT (Root Cause Analysis) forti che portano a misure correttive e preventive efficaci (CAPA).
Le registrazioni delle non conformità riguardano tutti gli scostamenti, rispetto ai requisiti stabiliti o agli accordi presi, evidenziati durante le attività lavorative sia in fase di progettazione che di esecuzione che di verifica del servizio fornito.
La procedura consente in particolare di:
✓ Indagare la non conformità rilevata
✓ definizione del trattamento immediato
✓ Identificare la causa principale mediante metodologie standardizzate quali 5 whys o Roote cause analisys a seconda della tipologia di Non conformità in oggetto
✓ Identificare le azioni da intraprendere per la risoluzione definitiva della stessa
✓ valutare se l'azione intrapresa determini effetti anche su processi contigui e valutarne l'eventuale impatto con la qualità del servizio erogato
✓ Implementare le azioni correttiva identificate
✓ Verificare l'efficacia dell'azione correttiva implementata
✓ Verificare che l'azione correttiva intrapresa possa essere implementata come azione preventiva anche in altri processi simili per evitare che la Non conformità rilavata possa ripresentarsi in altri processi.

Si allega la Procedura di Sistema PS 16 "NON CONFORMITA' - AZIONI CORRETTIVE - PREVENTIVE (CAPA)".

Valutazione : Accettabile
Commento di valutazione :

Le misure sono congrue.

Partizionamento

Il partizionamento non è possibile con REDCap.

Cifratura del disco contenente il database dell'applicativo effettuata mediante sistema cryptsetup-luks. Le caratteristiche dell'algoritmo sono le seguenti:

- Key: 512 bits Priority: normal Cipher: aes-xts-plain64 Cipher
- Key: 512 bits PBKDF: argon2id Hash: sha256

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Gestione del personale

La Fondazione eroga sistematicamente corsi di formazione in materia di cybersicurezza e protezione dei dati personali.

Valutazione : Accettabile
Commento di valutazione :
Le misure sono congrue.

Rischi

Accesso illegittimo ai dati

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

Accesso a dati anche relativi allo stato di salute da parte di soggetti non legittimati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Furto di password o di chiavi, Bug dovuti a software non aggiornato, Attacco hacker, Cessione di credenziali

Quali sono le fonti di rischio?

Sperimentatori del Centro, Terzi, Persone fisiche o software automatici, Personale del Centro Dati GIMEMA

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Sicurezza dell'hardware, Sicurezza dei siti web, Lotta contro il malware, Manutenzione, Pseudonimizzazione, Crittografia, Gestione del personale

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

Limitata, Limitata, vista la tipologia di dato trattato l'impatto sul possibile accesso illegittimo ai dati personali è limitato e richiede interventi in materia di sicurezza dei dati scelte con attenzione.

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

Limitata, Limitata. Valutate le misure di sicurezza logica e fisica adottate da GIMEMA nelle figure degli ADS e cloud provider (Seeweb srl), la possibilità di un accesso non autorizzato ai dati sensibili è limitato a bug non ancora riconosciuti o furto di password da parte degli utenti dei Centri, che accedono al database.
Con l'implementazione, nel 2022, del sistema di autenticazione a due fattori e la protezione dell'infrastruttura tramite VPN hardware, la probabilità del rischio risulta limitata.
Con l'attivazione, nel 2025, di un sistema SIEM (Security Information and Event Management) tramite il software Wazuh, è possibile monitorare e analizzare in tempo reale gli eventi di sicurezza:
- tutti gli accessi compresi quelli eventuali accessi non autorizzati o tentativi falliti
- segnalazione di aggiornamenti di sicurezza del sistema operativo e tutti i pacchetti installati al suo interno
La configurazione del sistema prevede degli alert in tempo reale via email per gli amministratori di sistema e il team di sicurezza, in modo da garantire una risposta tempestiva a potenziali minacce.

Valutazione : Accettabile
Commento di valutazione :

Allo stato attuale le misure risultano congrue.

Rischi

Modifiche indesiderate dei dati

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

Una modifica dei dati potrebbe comportare la verifica e la correzione dei dati da parte degli utenti del Centro sperimentatore., Nessun impatto per gli interessati

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

Fonti umane esterne, Errore dell'utente del Centro nella compilazione

Quali sono le fonti di rischio?

Attacco fraudolento al server da parte di hacker, Sperimentatori del Centro, Personale del Centro Dati GIMEMA

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

Controllo degli accessi logici, Sicurezza dei siti web, Lotta contro il malware, Sicurezza dell'hardware, Crittografia, Gestione del personale

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

Limitata, Limitata. Vista la tipologia di dato trattato l'impatto sul possibile accesso illegittimo ai dati personali è limitato e richiede interventi in materia di sicurezza dei dati scelte con attenzione.

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

Trascurabile, Trascurabile. Valutate le misure di sicurezza logica e fisica adottate da GIMEMA nelle figure degli ADS e del cloud provider (Seeweb srl) la possibilità del rischio è trascurabile.

In particolare, il sistema di raccolta dati registra tutte le attività degli utenti comprese l'inserimento, la modifica e cancellazione dei dati. Tali log permettono di ricostruire il dato in caso si verifichi una modifica indesiderata dei dati.

Valutazione : Accettabile
Commento di valutazione :

Allo stato attuale le misure risultano congrue.

Rischi

Perdita di dati

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

Qualora si verificasse una perdita dei dati gli utenti del Centro sarebbero costretti a re-inserire i dati nel database., Nessun impatto per gli interessati

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

Problemi hardware, Bug software

Quali sono le fonti di rischio?

Calamità naturali, Problemi tecnici cloud provider, Attacco hacker

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

Backup, Sicurezza dell'hardware, Manutenzione, Contratto con il responsabile del trattamento

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

Trascurabile, Trascurabile. La gravità del rischio è trascurabile in quanto i dati dei pazienti sono conservati nella documentazione originale, la cartella clinica, presente presso il Centro sperimentatore dove è in cura il paziente.

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

Trascurabile, Trascurabile. Le misure di backup, disaster recovery e mirroring messe in atto rendono remota l'incapacità di ripristinare i dati.
Da procedure interne il nostro R*ecovery Point Objective* (RPO) della *Business Continuity Plan* (BCP) è di 24 ore, in accordo con le nostre misure di backup e disaster recovery.

Valutazione : Accettabile
Commento di valutazione :

Allo stato attuale le misure risultano congrue.

Rischi

Panoramica dei rischi