Studi osservazionali [redacted] MPN0123

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

TO TRANSLATE - Validation

Mappaggio dei rischi

TO TRANSLATE - Validation

Piano d'azione

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

TO TRANSLATE - Validation

TO TRANSLATE - 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 DPO esprime parere favorevole sulla valutazione d'impatto effettuata dal Titolare, ritenendola condotta in conformità all'art. 35 GDPR ed alle indicazioni contenute nelle Linee Guida in materia di valutazione d'impatto adottate il 4 aprile 2017 dall' Article 29 Data Protection Working Party.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

In riferimento alla richiesta di parere agli interessati ai sensi dell'art. 35 par. 9 GDPR, il Titolare del trattamento ha considerato che – conformemente alle indicazioni contenute nelle Linee Guida in materia di valutazione d'impatto adottate il 4 aprile 2017 dall' Article 29 Data Protection Working Party- non ricorressero nel caso di specie le condizioni per chiedere le opinioni degli interessati sul trattamento previsto.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Gestione dei dati dei pazienti arruolati nell'ambito degli studi osservazionali [redacted] MPN0123 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 [redacted] MPN0123 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 solo 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 [redacted] MPN0123.

L'unico documento cartaceo contenente dati personali è il consenso informato dello studio 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 [redacted] MPN0123 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, come indicato nel protocollo scientifico studio specifico.

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 [redacted]MPN0123 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 alle seguenti aziende:
- BMS extra UE (USA) per lo studio MPN0123;
- Pfizer (stati non comunicati) per lo studio IFN0123;
- Janssen extra UE (UK e USA) per lo studio CLL2523.

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:
1. Connessione tramite VPN per accedere alla rete privata.
2. Accesso al server con chiave privata (SHA-256) in possesso esclusivo dell'ADS.
3. Accessi non corretti vengono bloccati dopo massimo 2 tentativi tramite il servizio fail2ban.

Recupero password
L'utente deve rispondere ad una domanda di sicurezza, impostata dall'utente al momento della configurazione dell'account, prima di poter richiedere il reset della password.

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 gli studi [redacted] MPN0123 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 utilizzate per accedere al sistema, così come della conservazione della propria password, ed è appositamento formato sulla relativa e specifica disciplina contenuta nell'apposito "Regolamento per l'utilizzo degli strumenti informatici".

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

Tracciabilità

I log del sistema operativo (Debian Linux) comprendono tutte le attività e accessi al server della piattaforma REDCap.
Parimenti i log degli accessi degli ADS nominati da Seeweb sono tracciati secondo le stesse modalità. L'accesso in modalità privilegiata viene registrato per eventuali verifiche di congruità. In aggiunta l'attività di amministrazione di sistema, ovvero le attività di accesso a privilegi elevati equiparabili, viene registrata su un log server specifico, le cui credenziali di accesso sono in possesso del Titolare e del Responsabile del trattamento di Seeweb.

L'accesso a tale sistema di collezione e di norma sottratto agli ADS, i quali potranno agire a seguito di autorizzazione del Titolare, ovvero del responsabile e solo per il tempo necessario allo specifico incarico. I dati verranno, inoltre, prelevati periodicamente e trasferiti su un supporto fisico persistente e non modificabile (cdrom).

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

Vulnerabilità

Gli accessi alla piattaforma REDCap sono protetti da password criptata nel database con chiave di criptatura.
Gli accessi al server per manutenzione, supporto e aggiornamento piattaforma e sistema operativo sono effettuati tramite chiave privata in possesso degli ADS, dopo connessione alla VPN privata.

Vengono installati, quando rilasciati, tutti gli aggiornamenti di sicurezza proposti dal sistema operativo (Linux Debian).

Il sistema di raccolta dati REDCap viene aggiornato ogni 6 mesi nella versione TLS (Long Time Support) dopo aver validato il corretto funzionamento dell'applicativo in un sistema di test.

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

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.

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

Lotta contro il malware

Le chiavi private per accesso ai server da parte degli ADS sono salvate in un file criptato protetto da password e utilizzate unicamente quando necessarie per accedere ai server.

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

Ai dati sono applicati i seguenti criteri di backup:

- backup realtime in mirroring;
- disaster recovery plan per il ripristino del sistema informatico.

Inoltre, è previsto un backup giornaliero per i server in produzione. il backup è settimanale per i server di disaster recovery.

Per le procedure di backup, verifica, disaster recovery ci si avvale dello specifico software TIVOLI TSM di IBM fornito da Seeweb srl.

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

Manutenzione

Si allega il documento "Certificazioni Seeweb" che descrive le certificazioni fornite da Seeweb.

Valutazione : Accettabile
Commento di valutazione :

Le misure sono congrue.

Protezione contro fonti di rischio non umane

Si allega il documento "Certificazioni Seeweb" che descrive le certificazioni fornite da Seeweb.

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.

Si allega il documento "Certificazioni Seeweb" che descrive le certificazioni in possesso del cloud provider.

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

Crittografia

La criptatura dei dati è limitata alla partizione contenente il database, in quanto è l'unica porzione del server nella quale sono presenti i dati sensibili.
La configurazione è a livello di sistema operativo con chiave di criptatura privata e in possesso degli ADS.

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.

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

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

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.

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

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

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, Protezione contro fonti di rischio non umane

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