

VALUTAZIONE D'IMPATTO PER PROGETTI DI RICERCA IN AMBITO SANITARIO

SU DATI RETROSPETTIVI PROSPETTICI

Informazioni Generali sullo Studio

La valutazione di impatto (DPIA) consente di identificare in modo puntuale i rischi per la protezione dei dati personali quando vengono pianificati nuovi progetti di ricerca o aggiornati progetti di ricerca in corso e di individuare le azioni necessarie per mitigare tali rischi.

Una valutazione di impatto, secondo l'Autorità Garante per la protezione dei dati personali, deve sempre essere effettuata negli studi retrospettivi quando:

- il trattamento dei dati personali è su larga scala;
- vengono trattate categorie particolari di dati, ad esempio dati genetici;
- l'attività comporta il data linkage di molteplici e diversi archivi di dati;
- l'attività prevede la rilevazione di dati per individui vulnerabili (minori, soggetti con patologie psichiatriche, anziani, ecc.);
- la base giuridica per il trattamento dei dati non è riferibile al consenso al trattamento, a ricerche condotte sulla base di disposizioni di legge o regolamento o al diritto, o ad altre specifiche fattispecie previste dal GDPR e dal Codice Privacy.

Identificativi dello Studio

A CURA DEL RICERCATORE

Titolare del Trattamento: Ospedale San Raffaele

Codice di Protocollo: ReteSLAC9

Titolo dello Studio: Titolo in Italiano: Registro di pazienti SLA con mutazione C9orf72 nella rete di 13 IRCCS "Istituto Virtuale Nazionale - Malattie del

Motoneurone (IVN-MMN)” Titolo in inglese: “Registry of ALS Patients with C9orf72 Mutation within the Network of 13 IRCCS of the ‘National Virtual Institute for Motor Neuron Diseases (IVN-MMN)

Sperimentatore Principale: Filippi Massimo

Unità: Neurologia

Data di Compilazione: 23/12/2025

Sinossi dello Studio: RAZIONALE La Sclerosi Laterale Amiotrofica (SLA) è una malattia neurodegenerativa a decorso fatale caratterizzata da progressiva degenerazione dei motoneuroni nell'encefalo e nel midollo spinale che conduce a paralisi degli arti, disfagia, disartria e insufficienza respiratoria, con esito finale di decesso per insufficienza respiratoria. La SLA insorge tipicamente nella tarda età media ed è caratterizzata da deficit motori progressivi che si sviluppano gradualmente nel corso di settimane, mesi o anni. Tale patologia ha una manifestazione clinica eterogenea e le basi biologiche di questa eterogeneità sono scarsamente comprese. L'insorgenza dei sintomi è tipicamente focale, ma la malattia si diffonde infine ad altre regioni del corpo. La sua progressione e diffusione sembrano essere invece sia locali che tra regioni neuroanatomiche collegate. Esistono due tipi di SLA differenziati dalla genetica: familiare e sporadica (idiopatica). Circa il 90% dei casi di SLA sono sporadici (SALS), mentre il restante 10% sono familiari (FALS). Un'espansione di ripetizioni esanucleotidiche (HRE) nel gene C9orf72 è responsabile del 30-50% dei casi di FALS, così come del 5-10% dei casi di SALS, e rappresenta il difetto genetico più comune nella SLA e nella demenza frontotemporale (FTD). La FTD rappresenta un gruppo di sindromi caratterizzate dal progressivo deterioramento del comportamento, del linguaggio e delle funzioni cognitive. Questa espansione nel gene C9orf72 è identificata come associata a uno spettro di caratteristiche fenotipiche complesse. Gli individui con SLA portatori della mutazione HRE C9orf72 (C9Pos) spesso mostrano tratti fenotipici diversi rispetto ai restanti pazienti (C9Neg), con una forma più aggressiva della malattia caratterizzata da una maggiore prevalenza di esordio bulbare, età di esordio più giovane e ridotta sopravvivenza. I casi C9Pos hanno anche una maggiore frequenza di comorbidità con la demenza frontotemporale (SLA-FTD) e una maggiore prevalenza di storia familiare di SLA e/o altre malattie neurodegenerative. Pertanto, la manifestazione clinica delle patologie associate a C9orf72, tipicamente definite come fenotipo SLA e fenotipo FTD, può variare da forme pure dell'una o dell'altra condizione, con molti fenotipi intermedi. È anche noto che circa il 35% dei pazienti con C9orf72 ha una presentazione atipica che imita altre malattie neurodegenerative e può portare a errori diagnostici. Avere una sintesi e una panoramica statistica delle caratteristiche di un'intera coorte di pazienti con SLA con C9orf72, prima di procedere con ulteriori studi di ricerca scientifica e clinica sulla SLA all'interno della rete IVN-MMN, può aiutare a chiarire la complessità clinica

della patologia da mutazione C9orf72 e la complessità del suo fenotipo correlato e della sua manifestazione. Attraverso questo registro (ReteSLAC9) intendiamo valutare gli aspetti chiave della patologia, come quelli relativi a 3 diversi fattori fenotipici (sede di insorgenza, fattori motori e fattori cognitivi) e al decorso clinico (attraverso il follow-up sui trattamenti necessari ricevuti). Valuteremo inoltre l'aspetto delle familiarità dei casi dei pazienti per la stessa SLA o per altre malattie neurodegenerative e le informazioni sull'ascendenza geografica paterna e materna, conferendo così al registro un importante potenziale anche come studio epidemiologico. Con l'inclusione continua di nuovi pazienti per tutta la durata del progetto della rete IVN-MMN, potremmo ottenere un Data-Base particolarmente importante a livello quantitativo e qualitativo, grazie al quale sarà possibile effettuare analisi statistiche sulla distribuzione di diversi parametri all'interno della popolazione e sulla relazione tra di essi, il che consentirà di comprendere, e fare piani, circa quali siano le direzioni di ricerca più promettenti nel contesto della SLA C9orf72.

OBIETTIVI 1. Avere, retrospettivamente, il dettaglio della popolazione di pazienti con SLA da mutazione C9orf72 al Tempo-zero di questo progetto 2. Valutare statisticamente le caratteristiche della coorte di pazienti nel Data-Base e proporre nuovi studi di analisi basati sulle statistiche effettuate 3. Aggiornamento prospettico dei dati attraverso il follow-up dei parametri del decorso clinico dei pazienti 4. Inclusione continua prospettica di nuovi pazienti nel Data-Base 5. Sulla base di tutte le analisi effettuate e dei risultati ed evidenze che potremmo portare alla luce, saremo in grado di acquisire informazioni su nuove possibili e fattibili linee di sviluppo della ricerca **ENDPOINT** Considerata soprattutto la rarità della condizione SLA C9orf72 in esame, i pazienti SLA C9orf72 e i soggetti pre-sintomatici C9orf72 che avranno firmato il consenso informato saranno aggiunti al registro ReteSLAC9 per tutta la durata del progetto di Rete Ministeriale IVN-MMN, con lo scopo di arricchire quanto più possibile il Data-Base su una condizione della quale si conosce ancora molto poco e sono necessari dati per far emergere prossime efficienti linee di ricerca. **METODOLOGIA** Per il supporto del registro ReteSLAC9 sarà utilizzata la piattaforma di collaborazione internazionale per la gestione sicura dei progetti di ricerca REDCap. I centri della rete IVN-MMN partecipanti al progetto avranno designato il loro personale di Data Entry al quale viene creato un account REDCap per l'inserimento dei dati estratti dalle cartelle cliniche. I dati saranno inseriti sempre in maniera anonimizzata, e non comprenderanno alcuna informazione sensibile, ed il personale del centro conserverà in maniera sicura e protetta la corrispondenza tra le identità dei soggetti ed i loro identificativi pseudonimizzati in REDCap (fondamentale per il follow-up prospettico). Ogni account REDCap visualizzerà soltanto i dati dei pazienti del proprio centro di appartenenza. I dati complessivi dei 13 centri della rete saranno raccolti centralmente dall'account di Project Manager del registro (Istituto Auxologico Italiano), che potrà solo visualizzare i dati in forma

pseudonimizzata senza alcuna possibilità di risalire alle identità dei soggetti degli altri centri. I 13 centri potranno scambiarsi i dati, sempre in forma pseudonimizzata, nelle fasi di analisi successive alla raccolta. Va ricordato infine che la raccolta comprenderà anche dati di pazienti deceduti retrospettivi. Questi, e i dati relativi a pazienti eventualmente deceduti, sono trattenuti perché ritenuti strategicamente utili per meglio inquadrare l'epidemiologia della popolazione di pazienti affetti dalla specifica mutazione in Italia in relazione al numero totale di pazienti affetti da SLA.

NUMERO DI SOGGETTI Come specificato il registro ReteSLAC9 si propone di raccogliere il massimo numero possibile di record di pazienti SLA C9orf72 e pre-sintomatici C9orf72 per tutta la durata del progetto di rete IVN-MMN. Al momento si è potuta comunque fare una stima sul potenziale complessivo attuale dei 13 centri di circa 200 soggetti.

CENTRI PARTECIPANTI o IRCCS Istituto Auxologico Italiano, Milano o Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico, Milano o Fondazione IRCCS Istituto Neurologico Carlo Besta o Centro Clinico NeMO - Fondazione Policlinico Universitario Agostino Gemelli IRCCS, Roma o IRCCS Eugenio Medea dell'Associazione "La Nostra Famiglia", Bosisio Parini (LC) o IRCCS Ospedale San Raffaele, Milano o Istituto delle Scienze Neurologiche IRCCS, Bologna o Ospedale Policlinico San Martino IRCCS, Genova o IRCCS Istituti Clinici Scientifici Maugeri, Pavia o IRCCS Istituto di Ricerche Farmacologiche Mario Negri, Milano o IRCCS Istituto Clinico Humanitas, Rozzano (MI) o IRCCS Fondazione Mondino, Istituto Neurologico Nazionale a Carattere Scientifico, Pavia o IRCCS Neuromed INM (Istituto Neurologico Mediterraneo), Pozzilli (IS)

DATA INIZIO E TERMINE DELLO STUDIO Data stimata inizio: 01/05/2025 Data stimata termine: 30/04/2028

POPOLAZIONE TARGET Maschi e femmine di età superiore a 18 anni con diagnosi di SLA e portatori di mutazione C9orf72 o pre-sintomatici (senza alcun sintomo) portatori di mutazione C9orf72.

CRITERI DI INCLUSIONE

1. Stato vitale ed essere attualmente seguito presso il relativo centro dell'IVN-MMN, oppure seguito e deceduto presso il relativo centro dell'IVN-MMN
2. Capacità di leggere e comprendere il contenuto del consenso informato e la natura dello studio (pazienti viventi)
3. Diagnosi di SLA e portatore della mutazione C9orf72 (C9Pos) o portatore della mutazione C9orf72 (C9Pos) senza manifestazioni cliniche (paziente pre-sintomatico)
4. Età ≥ 18 anni
5. Firma del consenso informato (pazienti viventi)

ASPETTI ETICI lo studio verrà condotto in accordo con le "Norme di Buona Pratica Clinica" definite a livello internazionale e nel rispetto dei principi etici stabiliti nella "Dichiarazione di Helsinki".

Modalità di Raccolta

Modalità di Raccolta Dati:

- direttamente presso l'interessato (paziente)
- da cartelle cliniche/documentazione sanitaria
- da archivi di dati clinici (esempio Dossier Sanitario Elettronico, RIS-PACS)
- da archivi di test diagnostici
- da database amministrativi
- da dati di laboratorio

Se Altro, specificare la modalità di raccolta:

Trattamento dei dati: Digitale (RedCap)

Se Altro, specificare tipologia di raccolta:

Categorie di Persone Interessate:

- Pazienti

Se Altro, specificare la categoria di persone:

Categorie di Dati Trattati:

- dati sulla salute fisica o psichica

Se Altro, specificare la categoria di dati trattati:

Dati Condivisi con Altri: SI

Ambiti di Comunicazione con altri: Promotore

Dati Trasferiti all'Estero: NO

Paesi Estero Coinvolti:

Misure di Protezione dei Dati

Dati Identificativi Conservati: SI

Se SI specificare le ragioni sottostanti a tale esigenza: I dati identificativi dei pazienti sono conservati esclusivamente presso i singoli centri partecipanti al fine di consentire il follow-up prospettico, l'aggiornamento dei dati clinici, la gestione del consenso informato e l'eventuale esercizio dei diritti dell'interessato, in conformità ai principi di minimizzazione e pseudonimizzazione dei dati.

Descrivere le procedure utilizzate per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca

Misure di Pseudonimizzazione:: Utilizzo di codici univoci per ciascun partecipante. Solo il responsabile della ricerca o altri soggetti autorizzati,

possono (con l'uso di mezzi ragionevoli) collegare i codici all'identità dei partecipanti

Se Altro, Specificare la procedura utilizzata per non identificare direttamente o rendere anonimi o pseudonimizzati i dati dei partecipanti nelle diverse fasi della ricerca:

Misure di Anonimizzazione: Altro

Se si utilizzano tecniche diverse dalla crittografia o utilizzo di codici univoci, specifica in dettaglio: Pseudoanonimizzazione. Il sistema assegnerà in automatico un codice ad ogni paziente registrato. Il singolo centro mantiene, in forma sicura e protetta, ed internamente al proprio team per l'IVN-MMN, il riferimento tra ogni codice di registro di REDCap e l'identificazione del loro relativo paziente.

PRINCIPI, FINALITA' E BASI GIURIDICHE

Necessità e proporzionalità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

☒ Sì ☐ No

Motivare la risposta:

- 1. Specificità degli scopi:** Gli scopi del trattamento sono chiaramente e analiticamente definiti all'interno del protocollo. In relazione agli obiettivi dello studio, il trattamento è legato esclusivamente alla ricerca così come dettagliatamente descritta e non a ulteriori scopi; pertanto, le finalità risultano circoscritte al contesto descritto. L'uso dei dati è confinato a uno scopo ben definito e non a fini generici o non correlati. Nella parte prospettica dello studio, oltre all'analisi di dati raccolti retrospettivamente, il protocollo prevede la raccolta di nuovi dati direttamente dagli interessati nel corso del follow-up clinico, attraverso visite di controllo programmate. La raccolta avviene nel rispetto delle finalità di ricerca dichiarate, senza estensioni indebite del trattamento.
- 2. Esplicitazione degli scopi:** Gli scopi del trattamento sono comunicati chiaramente negli endpoints del protocollo. Gli stessi sono funzionali a

raccogliere evidenze scientifiche, migliorare la comprensione delle patologie/trattamenti descritti, e i relativi dati saranno trattati in modo proporzionale all'obiettivo.

Per la parte prospettica dello studio la raccolta di dati in tempo reale permette di ottenere informazioni aggiornate, migliorando l'accuratezza delle analisi. Gli scopi della raccolta prospettica sono esplicitati nel modulo di consenso informato fornito ai partecipanti al momento dell'arruolamento, garantendo trasparenza e chiarezza sulle finalità del trattamento.

3. **Legittimità degli scopi:** Per quanto riguarda la legittimità, lo studio osservazionale deve rispettare i requisiti legali per la ricerca scientifica previsti dal GDPR e dalle normative nazionali applicabili. Poiché il trattamento è finalizzato alla ricerca, e non a scopi commerciali, rientra nelle finalità legittime ai sensi dell'art. 9 del GDPR, che consente il trattamento di dati sanitari per motivi di ricerca scientifica, soggetto all'adozione di adeguate misure di sicurezza e minimizzazione dei dati. Nella parte prospettica dello studio viene richiesto un consenso informato specifico agli interessati, conforme ai requisiti normativi, che autorizza l'uso dei nuovi dati raccolti nel corso dello studio. L'eventuale revoca del consenso comporterà l'interruzione della raccolta di dati prospettici, senza pregiudicare l'uso dei dati già raccolti nel rispetto delle disposizioni etiche e regolatorie.
4. **Proporzionalità e necessità:** Riguardo a proporzionalità e necessità, i dati trattati sono strettamente necessari a raggiungere gli obiettivi dello studio. Nel contesto di uno studio retrospettivo, ciò implica l'uso di dati già raccolti in precedenza, riducendo al minimo il rischio di interferenze non necessarie con la protezione dei dati degli interessati. L'utilizzo di dati anonimi o pseudonimizzati, ove applicabile, sarà sempre impiegato quale misura di mitigazione per limitare il rischio.
- Per la parte prospettica, la raccolta avviene nel rispetto del principio di minimizzazione, limitandosi ai dati essenziali per l'analisi scientifica e garantendo adeguate misure di sicurezza (es. pseudonimizzazione, accesso controllato ai dati).

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

☒ Sì ☐ No

Motivare la risposta: La valutazione circa la pertinenza, limitazione e necessità in relazione alle finalità dello studio in oggetto è basata sul principio di minimizzazione dei dati (art. 5(1)(c) del GDPR):

1. **Adeguatezza dei dati:** I dati raccolti sono appropriati per raggiungere le finalità dello studio. Nello studio osservazionale retrospettivo descritto, significa che i dati selezionati oggetto di trattamento sono strettamente necessari per rispondere ai quesiti oggetto della ricerca e alle ipotesi formulate nel protocollo. I dati trattati sono scelti in base alla loro rilevanza scientifica e clinica rispetto agli obiettivi dello studio. Per la parte prospettica, la raccolta di nuovi dati avviene in base a criteri predefiniti che garantiscono l'adeguatezza rispetto agli obiettivi della ricerca, senza raccogliere informazioni non pertinenti. I dati raccolti in tempo reale sono mirati a completare il set informativo necessario per rispondere agli endpoints dello studio.
2. **Pertinenza dei dati:** Nel contesto retrospettivo, vengono trattati solo i dati rilevanti rispetto agli obiettivi scientifici, evitando l'inclusione di informazioni non essenziali. Nel contesto prospettico, la selezione dei dati da raccogliere è basata sulla loro importanza rispetto agli outcome di ricerca. I dati raccolti durante il follow-up dei pazienti sono definiti a priori nel protocollo e devono rispondere a criteri chiari di pertinenza. In entrambi i casi, non vengono trattati dati che non abbiano una connessione chiara con le finalità dichiarate, limitando il trattamento alle informazioni essenziali per la validità scientifica dello studio.
3. **Limitazione dei dati (minimizzazione):** Il protocollo prevede la raccolta dei soli dati strettamente necessari per conseguire le finalità dello studio. Per lo studio retrospettivo, si utilizzano solo i dati pregressi indispensabili, selezionando accuratamente quelli rilevanti ed evitando informazioni ridondanti. Per lo studio prospettico, la raccolta è limitata a informazioni specifiche e necessarie per il monitoraggio nel tempo, escludendo dati eccessivi o non funzionali alla ricerca. In entrambi i casi, vengono adottate misure tecniche e organizzative per ridurre l'impatto sulla privacy degli interessati:
 - Pseudonimizzazione dei dati raccolti per limitare l'identificabilità diretta.
 - Controllo degli accessi ai dataset per prevenire trattamenti non autorizzati.
 - Meccanismi di verifica periodica per valutare la necessità della raccolta dati prospettica e, se necessario, limitare o interrompere la raccolta di informazioni non più essenziali.
4. **Necessità dei dati:** Relativamente al principio di necessità, lo studio non potrebbe essere condotto correttamente senza il trattamento dei dati previsti dal protocollo. Ogni categoria di dato trattato è necessaria per fornire risultati significativi e validi scientificamente. La raccolta di ulteriori

dati fuori protocollo non essenziali non sarebbe in alcun modo giustificata. Per la parte prospettica, la raccolta di nuovi dati è essenziale per monitorare l'evoluzione delle condizioni cliniche e valutare gli outcome nel tempo, garantendo la robustezza dei risultati scientifici. Pertanto, è possibile considerare i dati adeguati perché appropriati allo scopo dello studio, pertinenti perché direttamente legati alle finalità dichiarate e limitati in quanto raccolti solo nella misura strettamente necessaria per la ricerca, nel rispetto del principio di minimizzazione dei dati previsto dal GDPR.

Integrità ed esattezza

I dati sono esatti e aggiornati?

☒ Sì ☐ No

Motivare la risposta:

1. **Esattezza dei dati:** Lo studio osservazionale retrospettivo si basa su dati già esistenti, raccolti in precedenza per finalità cliniche. Poiché originariamente utilizzati per diagnosi e trattamenti medici, i dati sono stati raccolti e registrati con un alto livello di accuratezza e precisione, in quanto necessari per garantire la cura dei pazienti. Le fonti dei dati, quali ad esempio cartelle cliniche, referti o database ospedalieri, sono dunque affidabili in quanto strumentali al corretto trattamento del paziente, il che assicura una raccolta attenta e precisa delle informazioni.

Per la parte prospettica, i dati vengono raccolti in tempo reale secondo procedure standardizzate che ne garantiscono la qualità. La raccolta avviene seguendo criteri metodologici stabiliti nel protocollo dello studio, riducendo al minimo errori e discrepanze. In entrambi i casi, i dati trattati sono scelti in base alla loro qualità e rilevanza per la ricerca, evitando informazioni incomplete o imprecise.

2. **Validazione delle fonti dei dati:** Per i dati retrospettivi, le fonti sono istituzionalmente validate (es. cartelle cliniche, referti diagnostici, database ospedalieri) e soggette a controlli di qualità, garantendo la precisione delle informazioni.

Per i dati prospettici, la raccolta è effettuata secondo procedure predefinite con controlli immediati sulla correttezza dell'inserimento dei dati, come il double data entry o l'uso di strumenti elettronici certificati (eCRF – electronic Case Report Form).

3. **Controlli e verifiche incrociate:** Per garantire l'esattezza dei dati raccolti, vengono applicate le seguenti metodologie di controllo, adattate a ciascuna fase dello studio:

- Retrospectivo: Revisione e pulizia dei dati storici, con strumenti di data cleaning e analisi statistica per identificare anomalie. - Prospettico: Controllo immediato della qualità dei dati in fase di raccolta, con l'applicazione di procedure come audit trail, query management, risk-based monitoring e source data verification (SDV) per ridurre gli errori di trascrizione o inserimento.

4. Aggiornamento dei dati:

- Nel contesto retrospettivo, i dati utilizzati sono pertinenti per il periodo temporale dello studio e riflettono fedelmente la condizione clinica del paziente in quel determinato momento. Non necessitano di aggiornamenti in senso tradizionale, ma devono mantenere la loro coerenza con il periodo di riferimento. - Nel contesto prospettico, invece, i dati sono raccolti e aggiornati progressivamente nel tempo, in base al follow-up previsto. Eventuali nuove informazioni rilevanti per lo studio vengono integrate, garantendo che i dati siano sempre attuali rispetto agli obiettivi della ricerca.

5. Misure di mitigazione del rischio: Esclusivamente i dati accurati e affidabili vengano inclusi nelle analisi finali: lo studio adotta misure di mitigazione come l'esclusione di record non completi o poco chiari. Pertanto i dati trattati nello studio sono esatti perché raccolti da fonti affidabili e soggette a controlli di qualità, accurati nel contesto clinico originario e aggiornati rispetto al periodo storico di interesse. Inoltre, lo studio prevede misure per verificare la correttezza dei dati e garantire che qualsiasi eventuale errore venga identificato e corretto.

Durata di Conservazione dei Dati

Per quanto tempo verranno conservati i dati raccolti? 10 anni

Decorsa la data di conservazione i dati verranno: Anonimizzati completamente

Se Altro, specificare il destino dei dati:

Basi Giuridiche

Basi Giuridiche del Trattamento:

- art. 110, co. 1 primo periodo Codice Privacy

Motivi per cui non è possibile fornire l'informativa e acquisire il consenso:

MISURE A TUTELA DEI DIRITTI DELL'INTERESSATO

Informativa e consenso

Come sono informati del trattamento gli interessati?

È stata predisposta una valutazione di impatto ai sensi dell'art. 35 del GDPR?

È stata pubblicata la valutazione di impatto?

È stata comunicata l'avvenuta pubblicazione della valutazione al Garante Privacy?

Esercizio da parte dell'interessato dei diritti ex artt.15-22 DPR

È stata predisposta una procedura ad hoc da parte del Titolare? NO

Come fanno gli interessati a esercitare i loro diritti: Rivolgendosi direttamente ai titolari del trattamento o ai rispettivi dpo così come indicato nell'informativa.

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO

MISURA	Esistenti	Note
Organigramma interno	X	Ruoli e Responsabilità

Controllo accessi	X	L'accesso avviene tramite account personali. Sono applicate politiche di minimizzazione e restrizione dell'accesso ai dati personali. L'autenticazione è effettuata tramite password e, in alcuni casi, tramite autenticazione a due fattori. Sono adottate delle politiche di complessità delle password in coerenza con le buone pratiche di settore.
Gestione dei cambiamenti	X	Ogni modifica ai sistemi IT è valutata, registrata e monitorata. E' stata definita una procedura generale per la protezione dei dati personali, comprensiva di valutazioni in ottica by design e by default, volta a individuare i requisiti di protezione dei trattamenti e a implementare e mantenere i sistemi e le applicazioni garantendo livelli di sicurezza adeguati. L'acquisizione di componenti del sistema informativo tiene conto dei requisiti di sicurezza dei trattamenti che dovranno essere supportati e delle garanzie offerte dal fornitore.
Strumenti di sicurezza e protezione	X	Firewall, anti-malware centralizzati e strumenti di protezione per le postazioni di lavoro. Monitoraggio continuo del sistema IT per rilevare incidenti di sicurezza.
Gestione degli incidenti	X	Le violazioni dei dati personali vengono gestite tramite procedure di escalation, coinvolgendo il DPO. È attivo un sistema di monitoraggio continuo (SIEM e SOC) per

		raccogliere e analizzare i log. Il titolare mantiene un registro delle violazioni dei dati personali.
Rapporti con i Responsabili	X	Il titolare gestisce i rapporti con i propri Responsabili del trattamento attraverso accordi formalizzati che comprendono specifiche clausole per assicurare la riservatezza dei dati trattati e l'obbligo per i Responsabili di operare in conformità alla normativa sul trattamento dei dati personali, in particolare, per quanto riguarda le misure di sicurezza, in riferimento agli art. 28 e 32.
Pseudonimizzazione e cifratura	X	Pseudonimizzazione e cifratura sono utilizzate per limitare l'identificabilità dei dati. Viene applicata la cifratura nelle connessioni VPN, nei servizi HTTPS e nelle comunicazioni machine-to-machine.
Continuità operativa	X	L'infrastruttura IT è progettata per garantire la continuità operativa tramite due datacenter distanti almeno 20 km. I dati di backup sono conservati in un sito di recupero dati a oltre 100 km.

Formazione e gestione del personale	X	Il personale riceve formazione istituzionale con corsi FAD sulla protezione dei dati e sicurezza informatica, con incontri di aggiornamento periodici awareness e sensibilizzazione. Il personale con ruoli specifici nell'ambito della data protection (Local Privacy Executive e Local Privacy Contact) riceve una formazione specifica ulteriore.
Sicurezza delle postazioni di lavoro e delle reti	X	Le postazioni di lavoro sono aggiornate regolarmente e protette da sistemi anti-malware. Le reti sono protette da firewall e strumenti di monitoraggio delle intrusioni.
Backup e Vulnerability Assessment	X	Backup giornalieri dei dati e test periodici del sistema di ripristino. Valutazioni periodiche della vulnerabilità per identificare possibili rischi di sicurezza.
Sicurezza fisica	X	I datacenter sono protetti da misure fisiche e ambientali (protezione da incendi, allagamenti, controllo accessi fisici). I datacenter sono certificati TIER3 e TIER4.

VALUTAZIONE DEL RISCHIO

IMPATTO	PROBABILITA'
MASSIMO	4
IMPORTANTE	3
LIMITATO	2

TRASCURABILE

1

MATRICE DI VALUTAZIONE DEL RISCHIO

Probabilità (P)	Impatto (I)	Rischio (R=P*I)
Probabilità trascurabile: 1 Probabilità limitato: 2 Probabilità importante: 3 Probabilità massima: 4	Impatto trascurabile: 1 Impatto limitato: 2 Impatto importante: 3 Impatto massimo: 4	Rischio basso: $R < 6$ Rischio medio: $7 < R < 11$ Rischio alto: $R > 11$

Valutazione del Rischio

Accesso Illegittimo ai Dati: Importante

Modifiche Indesiderate dei Dati: Limitato

Perdita di Dati: Trascurabile

Valutazione Complessiva del Rischio: 15

Matrice di Valutazione del Rischio

 Description of Image

APPENDICE

MINACCE

ACCESSO ILLEGITTIMO AI DATI

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

Impatti Potenziali: Perdita di controllo dei propri dati. Utilizzo da parte di terzi di dati dell'interessato

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia: Comportamenti sleali/fraudolenti; Attacco informatico (es. social engineering, man in the middle, denial of service, brute force, etc.). Furto e/o perdita di dispositivi, supporti di memorizzazione, documenti

Quali sono le fonti di rischio?

Fonte: Fonti umane esterne (es. criminali informatici, fornitori, utenti). Fonti umane interne accidentali (es. collaboratori negligenti)

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Politiche di trasmissione dei dati; Crittografia; Pseudonimizzazione

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

Importante

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

Limitato

MODIFICHE INDESIDERATE DEI DATI

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

Impatti Potenziali: Dati non esatti e/o non aggiornati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Minaccia: Errore operativo

Quali sono le fonti di rischio?

Fonte: Fonti umane interne accidentali (es. collaboratori negligenti)

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

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti – intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Back – up dei dati

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

Limitato

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

Trascurabile

PERDITA DI DATI

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

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.

Impatti Potenziali

Costi aggiuntivi

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

Minaccia: Errore operativo

Quali sono le fonti di rischio?

Fonte: Eventi tecnologici (es. guasti, malfunzionamenti, etc.) Fonti umane interne accidentali (es. collaboratori negligenti)

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

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; Antivirus/firewall; Tracciabilità; Gestione postazioni; Politiche di tutela della privacy; Politiche di sicurezza informatica

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

Trascurabile

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

Trascurabile