DPIA – VIP SUL PROGETTO

"(Micro)RNA and informatics approaches for diagnosis, prognosis and treatment of Alzheimer's disease and Dementia - MYRIAD"

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

(VIP - DPIA)

CONTESTO

Motivazione della necessità di VIP/DPIA

La presente DPIA si pone come scopo quello di descrivere il trattamento dati effettuato nell'ambito del progetto di ricerca "(Micro)RNA and informatics approaches for diagnosis, prognosis and treatment of Alzheimer's disease and Dementia - MYRIAD" e di identificarne i rischi in relazione ai diritti e le libertà degli interessati. La stessa si rende necessaria in ossequio all'art. 110 co. 1, primo periodo, in combinato disposto con l'art. 110bis co. 4 del D. Lgs. 196/2003, come modificato dal D. Lgs. 101/2018 "Codice Privacy".

In particolare, il Titolare è accreditato quale Istituto di Ricovero e Cura a Carattere scientifico (IRCCS), tale da non costituire uso secondario l'utilizzo di dati personali già raccolti dallo stesso per finalità di cura in ossequi all'art. 110bis co. 4 Cod. Privacy.

Al momento della raccolta del campione, ad ogni modo, agli interessati è stato specificato che i dati personali ad esso associati sarebbero stati utilizzati per scopi di ricerca negli ambiti scientifici di interesse del Titolare (Disturbi psichici e/o neurodegenerativi).

Il presente progetto di ricerca, in conformità all'art. 110 D. Lgs. 196/2003 sopra richiamato, è stato oggetto, oltre che della presente valutazione di impatto, che verrà pubblicata sul sito istituzionale del Titolare all'indirizzo https://www.fatebenefratelli.it/ricerca-irccs-fatebenefratelli, nella sezione "Progetti di ricerca e documenti", anche di parere favorevole del Comitato Etico Territoriale competente (Lombardia 6), con n. di protocollo 0037823/24 dell'08/07/2024.

Le misure previste dal medesimo art. 110 verranno meglio descritte nel prosieguo della presente DPIA.

Panoramica del trattamento

Descrizione sistematica del trattamento e finalità.

Il contributo dell'IRCCS Istituto Centro San Giovanni di Dio Fatebenefratelli, afferente alla Provincia Lombardo Veneta dell'Ordine Ospedaliero San giovanni di Dio – Fatebenefratelli (quest'ultimo da intendersi quale Titolare del trattamento), nel progetto *"(Micro)RNA and informatics approaches for diagnosis, prognosis and treatment of Alzheimer's disease and Dementia (MyRIAD)"* (Cod. progetto: ERP-2023-23684212 – ERP-2023-JPND-MyRIAD), è quello di ricercare nuovi biomarcatori di neurodegenerazione associati ai miRNA e agli oxi-miRNA circolanti e all'interno delle vescicole extracellulari (Evs) nel siero. Nello specifico, l'IRCCS Fatebenefratelli (partner 4) parteciperà alla realizzazione di questo WP in qualità di WP leader e si occuperà dell'analisi di miR e oxi-miR nel siero e nelle Evs isolate da siero; della valutazione della concentrazione e dimensione delle Evs e della valutazione dei markers di neurodegenerazione/infiammazione, mitofagia e lisosomiali.
Presso il Laboratorio Marcatori Molecolari dell'IRCCS Istituto Centro San Giovanni di Dio Fatebenefratelli (partner 4), si effettueranno:

- L'isolamento dell'RNA seguito da small RNA-Seq sull'RNA totale (miRs), l'oxi-miR profiling a seguito di oxoG immunoprecipitation. I miR e oxi-miR (nel siero e nelle Evs) diversamente espressi verranno correlati con markers di neurodegenerazione, severità del

fenotipo (es. durata della malattia) e altri parametri clinici (es. familiarità per malattie neurodegenerative).

- La caratterizzazione delle Evs (dimensione e concentrazione) tramite Nanoparticle Tracking Analysis (NTA)
- La valutazione del contenuto all'interno delle Evs isolate da siero di:
  - (i) markers di neurodegenerazione e/o infiammazione (es. Nf-L, GFAP, UCH-L1, tau);
  - (ii) markers di autofagia/mitofagia (es. Pink1, Parkin);
  - (iii) markers lisosomiali (es. V-ATPasi).

Tali analisi saranno condotte su campioni raccolti in precedenza e conservati presso la biobanca dell'IRCCS Istituto Centro San Giovanni di Dio Fatebenefratelli (IRCCS FBF Biobank) (n=25 AD, n=25 FTD e n=25 controlli; coorte RNA-Seq).
Tali attività, in quanto effettuate su dati personali relativi a campioni biologici già conservati presso la biobanca IRCCS rappresentano un'operazione di trattamento dati ai sensi della definizione di cui all'art. 4 GDPR.
In particolare, i campioni analizzati sono identificati attraverso uno pseudonimo (codice progetto), che viene sovrapposto al già pseudonimo codice biobanca. Tale assetto fa sì che i suddetti dati non possano essere considerati anonimizzati per il Titolare, in quanto in possesso di tabelle di conversione.
Va sottolineato, comunque, come in nessuna fase del progetto di cui è DPIA i campioni ed i dati loro associati verranno trattati in chiaro o convertiti nei loro tratti identificativi.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del progetto è costituita dall'art. 110bis co. 4 del D. Lgs. 196/2003, da intendersi quale deroga al principio generale del consenso quale base giuridica sub art. 6 par. 1 lett. a del Reg. UE 679/2016 "GDPR".

Valutazione sulla necessità del trattamento dati e della sua proporzionalità.

Il trattamento dei dati personali è indispensabile per perseguire le finalità previste da progetto. Al fine del raggiungimento degli scopi di ricerca verranno utilizzati e trattati esclusivamente i dati personali strettamente necessari ad effettuare le analisi e le operazioni utili al perseguimento dello stesso, come meglio descritti nei seguenti paragrafi.

Dati, processi e risorse di supporto

Quali sono le categorie di dati trattati?

In associazione al codice progetto (come su specificato) verranno trattati dati personali comuni (sesso, età, scolarità) e particolari, ex art. 9 GDPR, nello specifico relativi allo stato di salute (diagnosi, età di esordio, durata della malattia, familiarità per malattie neurodegenerative, valutazioni neuropsicologiche es. MMSE e\o CDR).

Per il progetto verrà attribuito ad ogni campione proveniente da biobanca (già pseudonimizzato con un codice alfanumerico, "codice biobanca") un codice identificativo specifico ("codice progetto") che verrà utilizzato per tutta la procedura sperimentale e che, come anticipato, non verrà mai riconvertito in chiaro in nessuna fase del progetto.

Quali sono gli applicativi o altri strumenti con cui vengono trattati i dati?

I dati anagrafici, clinici e i dati generati dalle analisi previste da progetto sono conservati in files Excel (.xlsx). Nel dettaglio, le analisi sperimentali prevedono l'utilizzo dei seguenti strumenti, con relativi software, e generano le seguenti tipologie di file:

- - NextSeq 2000 Sequencing Systems (Illumina), NextSeq 1000/2000 Control Software – file FASTQ e file .csv/.xlsx;
- - NanoSight NS300 (Malvern Panalytical), NanoSight NTA 3.2 Software – file .nta, file video .avi e file .csv;
- - Simoa SR-X biomarker detection system (Quanterix), Software SRX 1.3 – file .csv;
- - Bio-Plex 200 System (Biorad), Bio-Plex Manager 6.0 – file .xlsx;
- - Lettore piastre ELISA Bio-Tek, KC4 3.4 Software – file KC4 data .pla e file .xlsx.

Qual è il periodo di conservazione dei dati?

I dati personali verranno conservati in coerenza con il periodo di conservazione previsto per i campioni della Biobanca e riportati nelle informative fornite agli interessati al momento della raccolta dei campioni, sotto riportata:

"*I Dati Personali riferiti ai campioni biologici verranno conservati, conformemente con l'applicazione delle misure di cui all'art. 89 GDPR, fino a quando essi saranno funzionali all'utilizzo in progetti di ricerca nell'ambito dei disturbi neurocognitivi e/o psichici*".

Modalità di conservazione e cancellazione dei dati

i dati personali trattati per le suesposte finalità verranno conservati:

- SUPPORTO INFORMATICO: I dati trattati su formati informatici ed elaborati attraverso gli applicativi suindicati verranno conservati in cartelle di rete con accesso riservato alla sola Unità di Ricerca assegnataria del presente progetto. Tali cartelle prevedono dei privilegi di accesso tale da impedire ad appartenenti ad altre Unità o a soggetti esterni l'accesso ai dati contenuti al suo interno. Gli unici soggetti esterni legittimati ad accedere sono gli amministratori di sistema debitamente nominati e solo in caso di necessità di assistenza o di richiesta da parte degli owner della cartella. I documenti contenuti all'interno delle cartelle riportano esclusivamente i codici progetto assegnati ai partecipanti allo studio. La tabella di conversione è conservata separatamente, protetta da password. Si ribadisce che la tabella di conversione non riporta in chiaro i dati identificativi dei partecipanti ma solo i codici biobanca cui sono associati gli specifici codici progetto. Le cartelle di rete come su descritte sono conservate/archiviate su server proprietari locali.

- SUPPORTO CARTACEO: i dati personali contenuti in supporti cartacei, quali possono essere stampe di originali informatici o documentazione cartacea raccolta presso i partecipanti, verranno conservati in armadi tenuti sotto chiave in locali anch'essi accessibili solo dai possessori delle chiavi (identificabili con gli stessi appartenenti all'Unità di Ricerca di cui sopra). Si tenga inoltre conto del fatto che l'intera area ricerca è accessibile solo da personale autorizzato e che la stessa, al di fuori dell'orario lavorativo è allarmata con apposito sistema.

Al termine del periodo di conservazione suindicato verranno cancellati/eliminati/distrutti a seconda del supporto su cui sono conservati.

Destinatari dei dati personali

Il Titolare condividerà dati esclusivamente con la University of Galway, in qualità di partner del progetto. La stessa Università si rende disponibile a fornire apposita informativa ex art 14 GDPR pubblicata sul proprio sito al fine di adempiere gli obblighi derivanti dalla normativa vigente.

I dati oggetto di condivisione saranno i risultati delle analisi di laboratorio effettuate sui campioni biologici conservati presso la biobanca dell'IRCCS. In particolare, giova sottolineare come i dati trattati da parte dell'IRCCS siano già pseudonimizzati e privi di dati identificativi. Una volta effettuate le analisi gli unici dati che verranno inviati al partner di ricerca saranno i risultati stessi, con esclusione di qualsiasi altro dato che non sia il solo "codice progetto" come sopra descritto

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

Al momento della prima stesura della presente DPIA, il progetto non prevede la nomina di Responsabili ex art. 28 GDPR.

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono specifici ed espliciti, contenuti in apposito protocollo di ricerca che ne individua le premesse, il contesto e gli scopi. Tali informazioni verranno rese note attraverso pubblicazione sul sito web del Titolare, nella sezione dedicata ai progetti di ricerca. Allo stesso modo il perseguimento degli scopi del progetto sono leciti nella misura in cui si inseriscono nel novero della ricerca medica, biomedica ed epidemiologica.

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

I dati raccolti, come indicati nell'apposito paragrafo, sono adeguati, pertinenti e limitati a quelli strettamente necessari per il perseguimento degli scopi di ricerca.

I dati sono esatti e aggiornati?

I dati trattati, basandosi su campioni biologici raccolti in un determinato momento, non richiedendo l'identificazione del campione, risultano essere esatti ed aggiornati in relazione alle finalità perseguite.

Misure a tutela dei diritti delle persone interessate

Come sono informati del trattamento le persone interessate?

In merito allo specifico progetto (MYRIAD) le persone interessate sono informate mediante apposita informativa privacy di progetto pubblicata sul sito IRCCS Fatebenefratelli, nella sezione dedicata ai progetti di ricerca.

Ove applicabile: come si ottiene il consenso delle persone interessate?

Il presente progetto, non effettuando un reclutamento attivo di partecipanti, ma limitandosi all'analisi di campioni già in possesso dell'IRCCS e conservati presso la sua Biobanca, non necessita del consenso al trattamento da parte degli interessati, sulla base dell'art. 110Bis co. 4 Cod. Privacy.

Come fanno le persone interessate a esercitare i loro diritti?

Il Titolare ha un'apposita procedura per l'esercizio dei diritti previsti dal GDPR in capo agli interessati. La stessa è contenuta nell'informativa pubblicata sul sito web del titolare, nella sezione dedicata ai progetti di ricerca.

La procedura è altrasì consultabile sul sito www.fatebenefratelli.it nella pagina "privacy", sezione "esercita i tuoi diritti privacy" ed è qui di seguito riportata.

*"Scaricando e compilando il modulo per l'esercizio dei diritti dell'interessato disponibile sul sito **www.fatebenefratelli.it** nella pagina "**privacy**", sezione "**esercita i tuoi diritti privacy**", Lei, seguendo le modalità indicate, può chiedere, in ogni momento:*

- *la revoca del consenso (art. 7 GDPR);*
- *l'accesso ai Dati che La riguardano (art. 15 GDPR);*
- *la loro rettifica ed integrazione (art. 16 GDPR);*
- *la cancellazione degli stessi (art. 17 GDPR). Nell'ambito della ricerca scientifica tale diritto può essere negato, nella misura in cui il suo esercizio rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento (art. 17 par. 3 lett. d GDPR);*
- *la limitazione del trattamento (art. 18 GDPR);*
- *la ricezione dei Dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico, nonché, di farli trasmettere ad altro titolare ("diritto alla portabilità dei Dati", art. 20 GDPR);*
- *di opporsi al trattamento (art. 21 GDPR).*

Si ricorda che in alcuni specifici casi previsti dal GDPR non tutti i sopracitati diritti sono esercitabili, in particolare (ma non limitatamente a) quando i trattamenti sono in esecuzione di obblighi di legge. In questi casi, sarà premura del Titolare, per mezzo delle risorse dedicate alla presa in carico della Sua richiesta di indicarLe i motivi ostativi all'esercizio dei diritti.

L'Interessato ha inoltre il diritto di proporre reclamo all'Autorità di controllo o di adire la competente Autorità Giudiziaria."

Il modulo così compilato potrà essere inviato alternativamente:

- via e-mail all'indirizzo dpo.plv@fatebenefratelli.eu;
- a mezzo di raccomandata indirizzata alla Provincia Lombardo Veneta dell'Ordine Ospedaliero di San Giovanni di Dio - Fatebenefratelli, Via Cavour n.22, 20063, CERNUSCO S/NAVIGLIO (MI), all'attenzione del Privacy Officer.

VALUTAZIONE DEI RISCHI

Calcolo del rischio (R)	**IMPATTO (I)**					
PROBABILITA' (P)		**Estremo**	**Significativo**	**Moderato**	**Lieve**	**Minimo**
	Imminente					
	Probabile					
	Possibile					
	Improbabile					
	Raro					

Legenda rischio (R)	
Alto	**Rischio non accettabile – da abbattere con priorità massima**
Medio-alto	**Rischio non accettabile – da abbattere**
Medio	**Rischio non accettabile – da mitigare**
Medio-basso	**Rischio accettabile – da monitorare**
Basso	**Rischio accettabile**

Legenda probabilità (P)
Imminente: con tutta probabilità l'evento è destinato a verificarsi in tempi brevissimi.
Probabile: vi è una buona possibilità che l'evento si verifichi a breve.
Possibile: è possibile che l'evento si verifichi.
Improbabile: questo tipo di evento è raro, ma c'è una reale possibilità che si possa verificare in futuro.
Raro: sebbene tale evento sia concepibile, probabilmente non si verificherà mai.

Legenda impatto (I)
Estremo: impatto di eccezionale gravità sui diritti e le libertà delle persone fisiche, eccezionalmente costoso e potenzialmente irrisolvibile.
Significativo: grave impatto operativo sui diritti e le libertà delle persone fisiche, estremamente costoso e difficilmente risolvibile.
Moderato: impatto operativo sui diritti e le libertà delle persone fisiche, molto costoso.
Lieve: impatto operativo limitato sui diritti e le libertà delle persone fisiche, alcuni costi.
Minimo: impatto minimo sui diritti e le libertà delle persone fisiche, costi trascurabili.

Calcolo rischio residuo (RR)
Il potenziale di attenuazione delle misure di sicurezza su P e/o I dev'essere valutato caso per caso dalla PLV, non potendo standardizzare tale valore.

Altri termini utilizzati
Categoria: Macro categoria che raccoglie più eventi, ha il solo scopo di categorizzare gli eventi.
Evento: oggetto dell'analisi dei rischi, accadimento capace di generare un impatto sui diritti e le libertà delle persone fisiche.
Vulnerabilità: accadimento che nel concreto è capace di generare l'evento (idealisticamente per ogni evento ci sono più vulnerabilità).
Conseguenza: tipo di impatto sui diritti e le libertà delle persone fisiche: perdita di integrità, perdita di disponibilità, perdita di riservatezza. In particolari casi sono prevedibili ulteriori conseguenze (es. difficoltà nell'esercizio dei diritti dell'interessato).

VALUTAZIONE DI RISCHIO INIZIALE SUPPORTI CARTACEI						
CATEGORIA	**EVENTO**	**VULNERABILITA'**	**CONSEGUENZA**	**I**	**P**	**R**
FORZA MAGGIORE	Incendio	Cortocircuito	Possibile perdita di disponibilità o integrità	Moderato	Improbabile	Medio-basso
	Allagamento	Blocco/rottura scarichi o tubature	Possibile perdita di disponibilità o integrità	Moderato	Improbabile	Medio-basso
	Fenomeni sismici	Terremoto	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni	Significativo	Improbabile	Medio
	Fenomeni atmosferici	Tromba d'aria, alluvione, nubifragio	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni	Significativo	Improbabile	Medio
	Deterioramento	Umidità, passare del tempo	Possibile perdita di disponibilità o integrità	Moderato	Possibile	Medio
ATTI DELIBERATI	Accesso non autorizzato (doloso)	Soggetto non autorizzato accede/sottrae dolosamente uno o più supporti fisici	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni	Significativo	Improbabile	Medio
	Intercettazione delle comunicazioni	Durante la trasmissione fisica di uno o più supporti un soggetto non autorizzato entra in possesso anche temporaneo dei dati trasmessi	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni /	Significativo	Improbabile	Medio
PROBLEMI ORGANIZZATIVI	Errore umano	Condivisione dei documenti con soggetti non autorizzati / mancato rispetto delle misure di sicurezza	Possibile perdita di riservatezza/disponibilità possibili discriminazioni /	Significativo	Possibile	Medio-alto
	Accesso non autorizzato (colposo)	Soggetto non autorizzato accede colposamente ai dati	Possibile perdita di riservatezza / possibili discriminazioni /	Moderato	Possibile	Medio

VALUTAZIONE DI RISCHIO RESIDUO SUPPORTI CARTACEI				
EVENTO	**VULNERABILITA'**	**M.S. ORGANIZZATIVE**	**M.S. TECNICHE**	**RR**
Incendio	Cortocircuito	Controlli periodici sugli impianti elettrici, estintori, presenza del team anti incendio, documenti chiusi in armadi, PR-PRY-003	Messa a terra, rilevatore di fumo	Basso
Allagamento	Blocco/rottura scarichi o tubature	Controlli periodici sugli impianti idraulici, documenti chiusi in armadi, PR-PRY-003	-	Basso
Fenomeni sismici	Terremoto	Documenti chiusi in armadi, PR-PRY-003	Edifici antisismici	Basso
Fenomeni atmosferici	Tromba d'aria, alluvione, nubifragio	Documenti chiusi in armadi, monitoraggio infissi, PR-PRY-003	-	Basso
Deterioramento	Umidità, passare del tempo	Documenti chiusi in armadi, monitoraggio infissi, PR-PRY-003	Uffici climatizzati	Basso
Accesso non autorizzato (doloso)	Soggetto non autorizzato accede/sottrae dolosamente uno o più supporti fisici	Documenti chiusi in armadi, uffici chiusi a chiave, controllo degli accessi alle strutture, PR-PRY-003	Videosorveglianza, allarme	Basso
Intercettazione delle comunicazioni	Durante la trasmissione fisica di uno o più supporti un soggetto non autorizzato entra in possesso anche temporaneo dei dati trasmessi	Autorizzazione al trattamento dei dati per tutto il personale che effettua il trattamento, formazione generale e specifica in tema protezione dati a tutto il personale, nomine a Responsabile del trattamento per tutti i fornitori, supporti cartacei trasmessi esclusivamente in busta chiusa all'interessato/delegato/soggetto autorizzato al trattamento/trasportatore esterno identificato e autorizzato, PR-PRY-003	Videosorveglianza	Basso
Errore umano	Condivisione dei documenti con soggetti non autorizzati / mancato rispetto delle misure di sicurezza	Autorizzazione al trattamento dei dati per tutto il personale che effettua il trattamento, formazione generale e specifica in tema protezione dati a tutto il personale, supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento, PR-PRY-003	-	Basso
Accesso non autorizzato (colposo)	Soggetto non autorizzato accede colposamente ai dati	Autorizzazione al trattamento dei dati per tutto il personale che effettua il trattamento, formazione generale e specifica in tema protezione dati a tutto il personale, documenti chiusi in armadi, documenti organizzati in archivi tematici, uffici chiusi a chiave	-	Basso

VALUTAZIONE DI RISCHIO INIZIALE SUPPORTI INFORMATICI						
CATEGORIA	**EVENTO**	**VULNERABILITA'**	**CONSEGUENZA**	**I**	**P**	**R**
FORZA MAGGIORE	Incendio	Cortocircuito	Possibile perdita di disponibilità o integrità	Moderato	Improbabile	Medio-basso
	Allagamento	Blocco/rottura scarichi o tubature	Possibile perdita di disponibilità o integrità	Moderato	Improbabile	Medio-basso
	Fenomeni sismici	Terremoto	Possibile perdita di disponibilità o integrità	Moderato	Improbabile	Medio-basso
	Fenomeni atmosferici	Tromba d'aria, alluvione, nubifragio	Possibile perdita di disponibilità o integrità	Moderato	Improbabile	Medio-basso
	Deterioramento	Umidità, passare del tempo	Possibile perdita di disponibilità o integrità	Moderato	Possibile	Medio
PROBLEMI TECNICI	Indisponibilità infrastruttura	Malfunzionamento dei sistemi, guasto impianto elettrico	Possibile perdita temporanea di disponibilità / possibile rallentamento nel riscontro agli interessati per l'esercizio dei loro diritti	Moderato	Possibile	Medio
INCIDENT (SERVIZI IT)	Bug	Un software o un altro strumento informatico presentano un malfunzionamento dovuto ad un'errata programmazione o ad una patch	Possibile perdita temporanea di disponibilità o riservatezza/ possibile rallentamento nel riscontro agli interessati per l'esercizio dei loro diritti	Moderato	Possibile	Medio
	Malware	Virus informatici di vario genere, tentativi di phishing di vario genere, scorretto utilizzo strumentazione aziendale	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni	Estremo	Possibile	Medio-alto
ATTI DELIBERATI	Intercettazione delle comunicazioni	Intercettazione "man in the middle"	Possibile perdita disponibilità, integrità e/o riservatezza / possibili discriminazioni	Estremo	Improbabile	Medio
	Accesso non autorizzato (doloso)	Consultazione/sottrazione dolosa di parte o dell'intero database o di uno strumento informatico	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni	Estremo	Possibile	Medio-alto
PROBLEMI ORGANIZZATIVI	Errore umano	Condivisione dei documenti con soggetti non autorizzati / mancato rispetto delle misure di sicurezza / scorretto utilizzo strumentazione aziendale	Possibile perdita di riservatezza, integrità, disponibilità / possibili discriminazioni	Significativo	Possibile	Medio-alto
	Accesso non autorizzato (colposo)	Soggetto non autorizzato accede colposamente ai dati	Possibile perdita di riservatezza / possibili discriminazioni	Moderato	Possibile	Medio

VALUTAZIONE DI RISCHIO RESIDUO SUPPORTI INFORMATICI				
EVENTO	**VULNERABILITA'**	**M.S. ORGANIZZATIVE**	**M.S. TECNICHE**	**RR**
Incendio	Cortocircuito	Controlli periodici sugli impianti elettrici, estintori, presenza del team anti incendio, PR-PRY-003, disaster recovery plan	Messa a terra, rilevatore di fumo, controllo della temperatura nella sala server, backup giornaliero (copertura 7 gg)	Basso
Allagamento	Blocco/rottura scarichi o tubature	Controlli periodici sugli impianti idraulici, PR-PRY-003, disaster recovery plan	Backup giornaliero (copertura 7 gg)	Basso
Fenomeni sismici	Terremoto	PR-PRY-003, disaster recovery plan	Edifici antisismici, backup giornaliero (copertura 7 gg)	Basso
Fenomeni atmosferici	Tromba d'aria, alluvione, nubifragio	Monitoraggio infissi, PR-PRY-003, disaster recovery plan	Backup giornaliero (copertura 7 gg)	Basso
Deterioramento	Umidità, passare del tempo	Monitoraggio infissi, PR-PRY-003, disaster recovery plan	Controllo della temperatura nella sala server, backup giornaliero (copertura 7 gg)	Basso
Indisponibilità infrastruttura	Malfunzionamento dei sistemi, guasto impianto elettrico	Fornitori servizi ICT tempestivamente coinvolti, disaster recovery plan	Backup giornaliero (copertura 7 gg), gruppo di continuità (2 ore)	Basso
Bug	Un software o un altro strumento informatico presentano un malfunzionamento dovuto ad un'errata programmazione o ad una patch	Fornitori servizi ICT tempestivamente coinvolti	-	Basso
Malware	Virus informatici di vario genere	Formazione generale e specifica in tema protezione dati a tutto il personale, autorizzazione al trattamento dei dati per tutto il personale, regolamento utilizzo strumenti informatici, PR-PRY-004, disaster recovery plan, PR-PRY-003, regolamento sull'utilizzo della strumentazione informatica	Firewall, antivirus, file ban, content filtering, sandbox, backup giornaliero (copertura 7 gg)	Basso
Intercettazione delle comunicazioni	Intercettazione "man in the middle"	Autorizzazione al trattamento dei dati per tutto il personale, formazione generale e specifica in tema protezione dati a tutto il personale, PR-PRY-003, PR-PRY-004	Crittografia in transito	Basso
Accesso non autorizzato (doloso)	Accesso/sottrazione dolosa di parte o dell'intero database o di uno strumento informatico	Controllo degli accessi alle strutture, PR-PRY-003, PR-PRY-004, uffici chiusi a chiave, switch fisico dedicato alla ricerca, cambio delle porte di connessione, blocco di porte non strettamente necessarie, regolamento sull'utilizzo della strumentazione informatica	Videosorveglianza, firewall, antivirus, allarme, backup giornaliero (copertura 7 gg)	Basso
Errore umano	Condivisione dei documenti con soggetti non autorizzati / mancato rispetto delle misure di sicurezza	Autorizzazione al trattamento dei dati per tutto il personale, formazione generale e specifica in tema protezione dati a tutto il personale, supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento, PR-PRY-003, PR-PRY-	-	Basso

		004, regolamento sull'utilizzo della strumentazione informatica		
Accesso non autorizzato (colposo)	Soggetto non autorizzato accede colposamente ai dati	Autorizzazione al trattamento dei dati per tutto il personale, formazione generale e specifica in tema protezione dati a tutto il personale, PR-PRY-004, regolamento sull'utilizzo della strumentazione informatica	-	Basso

Altre misure esistenti o pianificate

Il progetto di ricerca, cui si inserisce il trattamento dati per cui è DPIA, utilizza dati personali relativi a campioni biologici conservati nella Biobanca del Titolare. Va sin da subito reso noto come il servizio di Biobanca (in merito alla conservazione vera e propria dei campioni) è affidato in outsourcing alla Società SOL S.p.A.

Elemento da tenere inoltre in considerazione è il fatto che la società che eroga il servizio non ha alcun riferimento ai dati personali dei pazienti, ma solo un codice (codice biobanca) associato alla provetta contenente il campione biologico.

La tabella di conversione che associa il codice biobanca a nome, cognome e data di nascita del soggetto è conservata presso il Titolare. Si tratta di un file protetto da password, che viene cambiata mensilmente e che è nota solo ai membri del Servizio Biobanca. Il file è conservato in cartella di rete con accesso riservato al solo Servizio Biobanca. Come descritto in precedenza, le cartelle prevedono dei privilegi di accesso tale da impedire ad appartenenti ad altre Unità o a soggetti esterni l'accesso ai dati contenuti al suo interno. Gli unici soggetti esterni legittimati ad accedere sono gli amministratori di sistema debitamente nominati e solo in caso di necessità di assistenza o di richiesta da parte degli owner della cartella. Le cartelle di rete come su descritte sono conservate/archiviate su server proprietari locali.

A tal fine si ritiene opportuno qui delineare le misure tecniche ed organizzative poste in atto a tutela dei diritti e le libertà degli interessati basate sulle informazioni concesse dalla SOL S.p.A.

VALUTAZIONE DI RISCHIO INIZIALE BIOBANCA						
CATEGORIA	**EVENTO**	**VULNERABILITA'**	**CONSEGUENZA**	**I**	**P**	**R**
FORZA MAGGIORE	Incendio	Cortocircuito	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Improbabile	Medio
	Allagamento	Blocco/rottura scarichi o tubature	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Improbabile	Medio
	Fenomeni sismici	Terremoto	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Improbabile	Medio
	Fenomeni atmosferici	Tromba d'aria, alluvione, nubifragio	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Improbabile	Medio
	Deterioramento	Umidità, passare del tempo	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Possibile	Medio-alto

PROBLEMI TECNICI	Indisponibilità infrastruttura	Malfunzionamento dei sistemi, guasto impianto elettrico	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Possibile	Medio-alto
ATTI DELIBERATI	Intercettazione delle comunicazioni	Durante il trasporto di uno o più campioni biologici un soggetto non autorizzato entra in loro possesso anche temporaneamente	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Possibile	Medio-alto
	Accesso non autorizzato (doloso)	Sottrazione dolosa di uno o più campioni biologici	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici	Significativo	Possibile	Medio-alto
PROBLEMI ORGANIZZATIVI	Errore umano	Condivisione dei campioni biologici con soggetti non autorizzati / recapito dei campioni biologici ad un diverso Titolare del trattamento / mancato rispetto delle misure di sicurezza	Possibile perdita di disponibilità, integrità e inalterabilità dei campioni biologici / possibili discriminazioni / possibili eventi di angoscia o depressivi	Estremo	Possibile	Medio-alto

VALUTAZIONE DI RISCHIO RESIDUO BIOBANCA				
EVENTO	**VULNERABILITA'**	**M.S. ORGANIZZATIVE**	**M.S. TECNICHE**	**RR**
Incendio	Cortocircuito	Impianti elettrici realizzati a regola d'arte, estintori a polvere, presenza del team anti incendio, istruzioni in caso di perdite di campione biologico, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Messa a terra, rilevatore di fumo, sistema anti-incendio, controllo della temperatura	Basso
Allagamento	Blocco/rottura scarichi o tubature	Controlli periodici sugli impianti idraulici, istruzioni in caso di perdite di campione biologico, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Monitoraggio umidità	Basso
Fenomeni sismici	Terremoto	Campioni biologici conservati in aree fisicamente protette, istruzioni in caso di perdite di campione biologico, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach		Basso
Fenomeni atmosferici	Tromba d'aria, alluvione, nubifragio	Campioni biologici conservati in aree fisicamente protette, istruzioni in caso di perdite di campione biologico, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Monitoraggio umidità	Basso
Deterioramento	Umidità, passare del tempo	Campioni biologici conservati in aree fisicamente protette, controlli anti-parassitari/derattizzazione, servizio di pulizia, istruzioni in caso di perdite di campione biologico, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Controllo temperatura, monitoraggio umidità e atmosfera interna, sistema di areazione	Basso

Indisponibilità infrastruttura	Malfunzionamento dei sistemi, guasto impianto elettrico	Impianti elettrici realizzati a regola d'arte, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Gruppi di continuità	Basso
Intercettazione delle comunicazioni	Durante il trasporto di uno o più campioni biologici un soggetto non autorizzato entra in loro possesso anche temporaneamente	Autorizzazione al trattamento e formazione di tutti i dipendenti, trasporto sicuro dei campioni biologici tramite contenitori e mezzi che assicurino la disponibilità, l'integrità, la provenienza e l'inalterabilità dei campioni biologico e la riservatezza dell'interessato; SOL S.p.A. non è in possesso delle anagrafiche degli interessati; non vengono utilizzati trasportatori terzi, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Automazione delle richieste di consegna e ritiro di campioni biologici	Basso
Accesso non autorizzato (doloso)	Sottrazione dolosa di uno o più campioni biologici	Autorizzazione al trattamento e formazione di tutti i dipendenti, controllo degli accessi biometrico, accesso riservato al solo personale previamente autorizzato, politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Videosorveglianza h24 7 giorni su 7	Basso
Errore umano	Condivisione dei campioni biologici con soggetti non autorizzati / recapito dei campioni biologici ad un diverso Titolare del trattamento / mancato rispetto delle misure di sicurezza	Autorizzazione al trattamento e formazione di tutti i dipendenti, trasporto sicuro dei campioni biologici tramite contenitori e mezzi che assicurino la disponibilità, l'integrità, la provenienza e l'inalterabilità dei campioni biologico e la riservatezza dell'interessato; SOL S.p.A. non è in possesso delle anagrafiche degli interessati; non vengono utilizzati trasportatori terzi, controllo degli accessi biometrico, accesso riservato al solo personale previamente autorizzato; politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach	Automazione delle richieste di consegna e ritiro di campioni biologici	Basso

Gestione del personale

Il trattamento dei dati personali per il presente progetto di ricerca verrà effettuato esclusivamente dall'Unità di Ricerca "*Marcatori Molecolari*" sotto la diretta vigilanza e responsabilità del PI dott.ssa Roberta Ghidoni e dal personale del Servizio di Statistica del comparto ricerca dell'IRCCS.

Come anticipato nel par. relativo alle modalità di conservazione dei dati gli unici soggetti esterni autorizzati ad accedere direttamente ai dati di ricerca possono essere gli amministratori di sistema per assistenza tecnica richiesta dall'Unità di Ricerca titolare.

Si rende noto che tutto il personale del Titolare è stato debitamente autorizzato al trattamento dei dati personali ex art. 2quaterdecies del D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018.

PARERE DEL DPO

La presente valutazione di impatto è stata redatta con il contributo delle unità operative coinvolte nel trattamento e dall'Ufficio Privacy della PLV – Fatebenefratelli, sotto la supervisione del DPO.

Data prima versione 04/11/2024.