VALUTAZIONE GENERALE D'IMPATTO SULLA PROTEZIONE DEI DATI RIGUARDO L'ATTIVITA' DI RICERCA MEDICA, BIOMEDICA ED EPIDEMIOLOGICA ESEGUITA DALL'IRCCS ISTITUTO CENTRO SAN GIOVANNI DI DIO FATEBENEFRATELLI

1	Prima Emissione	Moccia	Sammartino Ghidoni Bellini Porteri Ienco	-	Baldo	07/10/2025
VER.	**MOTIVO**	**ELAB.**	**VER.**	**CONT.**	**APPR.**	**DATA**

Indice

1. Intenti del Titolare del trattamento

La Provincia Lombardo Veneta dell'Ordine Ospedaliero di San Giovanni di Dio – Fatebenefratelli (di seguito "il Titolare" o "la PLV") è l'ente controllante l'IRCCS Istituto Centro San Giovanni di Dio Fatebenefratelli di Brescia (di seguito "IRCCS").

L'IRCCS (come da sua principale funzione riconosciuta dal d.lgs. 288/03) svolge numerose attività di ricerca scientifica in ambito medico, biomedico ed epidemiologico all'interno delle varie unità di ricerca.

La PLV ha provveduto a nominare un Data Protection Officer in ossequio all'obbligatorietà di tale nomina, come si evince dall'art. 37, comma 1, lett. c) del GDPR. Il DPO è contattabile all'indirizzo dpo.plv@fatebenefratelli.eu

Il Titolare del trattamento, con il presente documento, intende svolgere una valutazione generale degli impatti sulla protezione dei dati personali ("DPIA Generale") relativa all'attività di ricerca scientifica in ambito medico, biomedico ed epidemiologico, con la premessa che tale valutazione prenderà in considerazione esclusivamente gli elementi comuni delle varie attività di ricerca, rimandando a documenti specifici nel caso in cui fosse necessario eseguire degli approfondimenti ad hoc.

1.1. Analisi sull'obbligatorietà di svolgimento della DPIA

Al fine di valutare l'obbligatorietà di svolgimento di una valutazione d'impatto sulla protezione dei dati personali (art. 35 del GDPR), apposita procedura interna (Procedura PR-PRY-005 - gestione del processo di valutazione dei rischi privacy e DPIA PLV) indica come criterio di riferimento quello proposto dal WP29 con le Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 come modificate e adottate da ultimo il 4 ottobre 2017.

Elementi	Presente? (SI/NO)
1) Evalutation or scoring, compresa la profilazione e le attività predittive (anche su aspetti riguardanti il rendimento professionale)	**NO**
2) Decisioni automatizzate che producono effetti giuridici o incidono significativamente sugli interessati	**NO**
3) Monitoraggio sistematico	**NO**
4) Dati sensibili di natura estremamente personale	**SI**
5) Trattamenti su larga scala	**NO**
6) Combinazione o raffronto di insiemi di dati	**NO**
7) Dati relativi a soggetti vulnerabili	**SI**

8) Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o innovative	**NO**
9) Trattamenti che possono impedire agli interessati di esercitare i propri diritti o avvalersi di servizi o di un contratto	**NO**

Considerando che il WP29 (e la procedura interna sopra indicata) indica, come linea generale, che l'obbligatorietà della DPIA scatti in presenza di almeno due di questi elementi, ma che in determinati casi se ne possa valutare l'opportunità di svolgimento anche in presenza di uno solo di questi, il Titolare del trattamento non ha dubbi nel dichiarare che, per l'attività di ricerca in ambito medico, biomedico ed epidemiologico lo svolgimento di una valutazione d'impatto sulla protezione dei dati sia sempre necessaria.

L'effettiva sussistenza degli elementi segnalati (dati sensibili di natura estremamente personale e dati relativi a soggetti vulnerabili) verrà dimostrata al paragrafo 3 "Attività di trattamento di dati personali".

L'elemento "utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o innovative" si riscontra esclusivamente nelle ipotesi meglio descritte ai punti 2.3.3. e 2.3.5.

L'elemento "combinazione o raffronto di insieme di dati" si riscontra esclusivamente nell'ipotesi meglio descritta al punto 2.3.4.

L'elemento "trattamenti su larga scala" si riscontra esclusivamente nell'ipotesi meglio descritta al punto 2.3.4.

1.2. Laboratori, unità e servizi di ricerca dell'IRCCS

L'Unità Operativa di Psichiatria si occupa di valutare e implementare percorsi terapeutici per pazienti con disturbi mentali e i loro familiari e di promuovere interventi di prevenzione rivolti alla popolazione giovanile. Inoltre, l'UO promuove studi volti ad individuare i correlati clinici, biologici e cerebrali associati alla diagnosi e alla risposta al trattamento, con particolare riferimento al Disturbo Borderline di Personalità, e di potenziali fattori di rischio transdiagnostici legati alla malattia mentale, come la disregolazione emotiva.

L'Unità Operativa di Psichiatria Epidemiologica e Digitale lavora sulle seguenti aree tematiche nell'ambito della salute mentale: (1) epidemiologia dei disturbi mentali e dei fattori di rischio, ed health services research; (2) impiego di strumenti digitali in salute mentale per il monitoraggio dell'attività fisica e del ritmo sonno-veglia, e per la rilevazione in tempo reale di dati fenotipici ed esperienziali (Ecological Momentary Assessment); (3) salute mentale dei giovani, e transizione assistenziale dai servizi di psichiatria dell'infanzia/adolescenza ai servizi per l'età adulta; (4) comorbilità fisiche in persone con disturbi mentali; (5) psichiatria forense.

L'Unità Operativa di Neuropsicologia si occupa di sviluppare e armonizzare protocolli di studio delle principali funzioni cognitive e della loro variazione nell'invecchiamento cerebrale fisiologico e patologico. Inoltre, altro focus è lo sviluppo di approcci innovativi nella riabilitazione delle funzioni cognitive, e l'applicazione di metodiche di stimolazione cerebrale non invasiva, riabilitazione neuropsicologica e teleriabilitazione cognitiva.

L'Unità Operativa Neurofisiologia si occupa di sviluppare nuovi marcatori neurofisiologici di patologie psichiatriche e neurodegenerative, attraverso l'utilizzo di un approccio innovativo e multimodale che permette di ottenere misurazioni di reattività corticale e di connettività cortico-corticale e di valutare il potenziale terapeutico delle tecniche non invasive di stimolazione cerebrale in pazienti affetti da patologie psichiatriche e dementigene.

L'Unità Operativa di Neuroimmagine e Epidemiologia Alzheimer si focalizza su studi volti a comprendere l'organizzazione funzionale del cervello e i meccanismi patofisiologici sottostanti i disturbi neurocognitivi e le malattie mentali attraverso tecniche avanzate di neuroimmagine.

L'Unità Operativa di Neuroinformatica si occupa di sviluppare piattaforme e servizi web-based (e.g.: neuGRID, NewPsy4u) per l'analisi di segnali cerebrali e una medicina personalizzata. In particolare, si occupa di gestire Big-Data multimodali per lo sviluppo di strumenti di intelligenza artificiale (AI) per favorire una caratterizzazione profonda (deep-phenotyping) delle demenze e malattie mentali.

Il Laboratorio di Genetica studia la variabilità genetica, con tecnologie di sequenziamento di nuova generazione (NGS) su varianti comuni, mutazioni note e nuove varianti rare, associata alle patologie psichiatriche e ai loro endofenotipi al fine di identificare nuovi target/biomarcatori implicati nella efficacia delle terapie farmacologiche e non farmacologiche.

Il Laboratorio di Marcatori Molecolari studia le basi molecolari delle malattie mentali e in particolare dei disturbi neurocognitivi (dovuti a degenerazione frontotemporale, Malattia di Alzheimer e a corpi di Lewy) caratterizzati non solo da danno organico cerebrale sottostante, ma frequentemente anche da importanti manifestazioni comportamentali e psichiatriche. Nello specifico - mediante l'impiego di tecnologie ad alta produttività/sensibilità (e.g. saggi multiparametrici, spettrometria di massa, NTA, NGS) – il Lab si occupa dello studio di biomarcatori molecolari per la diagnosi precoce e differenziale, di nuovi determinanti genetici, fattori di rischio e modulatori genetici/epigenetici di malattia.

Il Laboratorio di Psichiatria Biologica studia i meccanismi molecolari associati allo sviluppo delle principali malattie psichiatriche, in particolare depressione life time e perinatale, e alla risposta al trattamento. Principale interesse è volto all'interazione tra eventi stressanti (soprattutto quelli nei primi anni di vita), sistema infiammatorio, sistema di risposta allo stress e il microbiota intestinale mediante approcci sia OMICI che di "gene/pathway candidato". Si occupa di valutare come questi sistemi biologici siano coinvolti non solo nello sviluppo della malattia, ma anche nell'efficacia di interventi farmacologici con antidepressivi o non farmacologici come esercizio fisico o dieta. Fine ultimo è l'identificazione di biomarcatori periferici che possano essere associati al rischio di malattia, alla progressione e predittori della risposta.

L'Unità Operativa di Riabilitazione Alzheimer si focalizza sulla diagnosi e terapia delle diverse forme di demenza, sull'esecuzione di esami neurofisiologici e su studi relativi ai marcatori clinici associati all'insorgenza e progressione della malattia di Alzheimer, approfondendo la correlazione tra indici clinici, biologici e funzionali.

L'Unità di Bioetica svolge le seguenti principali attività: 1) studio delle questioni bioetiche della ricerca e della cura relative a soggetti con impedimento cognitivo e disordine psichiatrico in un contesto di incrementata conoscenza e possibilità di intervento; 2) supporto nella scrittura e conduzione di progetti di ricerca che garantiscano e promuovano i diritti e il benessere dei soggetti partecipanti, con specifica attenzione alle popolazioni vulnerabili; 3) coordinamento delle attività del Comitato etico Fatebenefratelli, organismo consultivo di riferimento per le strutture della Provincia Lombardo Veneta dei Fatebenefratelli; 4) attività di raccordo tra l'IRCCS Fatebenefratelli e il Comitato etico CET 6 di Regione Lombardia per la valutazione dei protocolli di ricerca.

La Clinical Trial Unit (CTU) si occupa della organizzazione e pianificazione degli studi interventistici farmacologici e non-farmacologici, operando mediante standard qualitativi richiesti dagli enti regolatori. In particolare, la CTU supporta i ricercatori dell'Istituto nella revisione della sinossi e della fattibilità degli studi interventistici profit e non-profit, nel rapporto con i Comitati Etici, nella gestione dei pazienti reclutati e nel monitoraggio e archiviazione dei dati.

Il Servizio Biobanca svolge le seguenti principali attività: 1) archiviazione e mantenimento del materiale depositato in Biobanca; 2) gestione del database dedicato; 3) archiviazione della documentazione inerente ai campioni depositati in Biobanca; 4) monitoraggio flusso materiale biologico in ingresso ed in uscita; 5) messa in rete con Biobanche nazionali e internazionali.

Il Servizio Statistica si occupa dell'elaborazione statistica dei dati inerenti alla ricerca scientifica (applicazione di metodi e modelli statistici in ambito epidemiologico, bioinformatico e neuroimaging); il servizio collabora inoltre alla stesura di progetti scientifici (pianificazione del disegno sperimentale, definizione del piano di campionamento, scheduling della procedura di analisi) e all'implementazione di tools statistico-computazionali per la traslazionalità clinica dei risultati della ricerca.

Il Servizio Biblioteca svolge le seguenti attività: 1) servizio di *reference* e formazione agli utenti di Istituto con corsi individuali o a piccoli gruppi e partecipazione a *webinar* con formatori esterni; 2) ricerche bibliografiche su banche dati; 3) *document delivery* e prestito interbibliotecario; 4) gestione e rinnovi dei periodici in abbonamento; 5) ricerca e calcolo valori bibliometrici (e.g. Impact Factor, H-Index); 6) tenuta Pubblicazioni istituzionali con rispettiva rendicontazione annuale al Ministero della Salute tramite inserimento dei dati nel Workflow della Ricerca con utilizzo del software *Pure*; 7) invio newsletter.

Il Servizio Trasferimento Tecnologico svolge le seguenti principali attività: 1) ricerca e sviluppo di soluzioni innovative e applicazioni pratiche per una valorizzazione dei risultati della ricerca; 2) gestione della proprietà intellettuale, favorendo la promozione di innovazioni tramite brevetti; 3) attività di scouting delle opportunità di finanziamento e per la costituzione di partenariati di valorizzazione della ricerca.

L'Ufficio Ricerca supporta la Comunità Scientifica dell'IRCCS: 1) nell'individuazione delle opportunità di finanziamento per la ricerca in ambito nazionale ed internazionale attraverso le attività di scouting, valutazione di pre-fattibilità e sottomissione dei progetti agli Enti finanziatori; 2) nella gestione amministrativa con la redazione di documenti e contratti (verso Ente finanziatore e partner di progetto) e per la finalizzazione del sostegno; 3) nella gestione economica dei finanziamenti ottenuti (ricezione delle richieste di acquisto materiali di consumo, strumentazioni e servizi a scopo di Ricerca e gestione del ciclo approvativo di spesa); 4) nella rendicontazione dei finanziamenti. Svolge altresì attività istituzionali di supporto: 5) alla Direzione Scientifica quali ad esempio gestione e rendicontazione finanziamenti istituzionali (ricerca corrente, 5xmille), raccolta della documentazione per la conferma del carattere scientifico; 6) alla Direzione Amministrativa quali ad esempio gestione flussi contabili con la presentazione dei dati economici per la chiusura di bilancio.

2. L'attività di ricerca medica, biomedica ed epidemiologica

Presso l'IRCCS vengono eseguite le seguenti tipologie di ricerca medica, biomedica ed epidemiologica: studi osservazionali prospettici e retrospettivi, studi interventistici di tipo diverso, incluse le sperimentazioni cliniche di farmaci.

In considerazione della complessità organizzativa dell'area ricerca dell'IRCCS (vedi punto precedente) e considerate le peculiarità del lavoro delle varie unità di ricerca (essenziali per l'ottimizzazione e l'efficientamento delle loro quotidiane attività, ma di scarso interesse per le finalità del presente documento) la PLV ha eseguito l'analisi che segue sforzandosi di generalizzare il più possibile, senza perdere di valore descrittivo, i vari passaggi dell'attività di ricerca medica, biomedica ed epidemiologica.

2.1. Raccolta dei dati di ricerca

Le modalità di raccolta dei dati di ricerca dipendono essenzialmente da due elementi: Il tipo di ricerca che si intende eseguire e l'organizzazione del progetto di ricerca.

2.1.1. Arruolamento dei partecipanti

In una buona parte dei progetti di ricerca si deve procedere all'arruolamento dei partecipanti direttamente presso l'IRCCS, questo può avvenire con varie modalità:

- Pubblicizzazione della ricerca: la ricerca viene presentata e pubblicizzata in vari modi, e principalmente tramite il sito web, opuscoli, riunioni e lezioni pubbliche e tramite il passa parola (in maniera informale e non organizzata);
- Contatto e proposta diretta: presso l'area ricerca dell'IRCCS si tiene traccia, nei documenti di conversione (vedi punto 3.6.), dei consensi al ricontatto per eventuali ricerche future;
- Offerta diretta di partecipazione ai caregiver dei pazienti: durante i vari contatti con i caregiver dei pazienti, qualora risultasse pertinente, le varie unità di ricerca illustrano il progetto e propongono la partecipazione;
- Proposta diretta di partecipazione nei vari servizi dell'istituto: presso ambulatori, Mac e comunità residenziali vengono presentati i vari progetti di studio e viene proposta ai pazienti la partecipazione (in ragione della categoria di partecipante prevista dal progetto di studio).

2.1.2. Selezione dalle cartelle cliniche

La selezione dei dati di ricerca dalle cartelle cliniche è prospettabile per gli studi retrospettivi e prospettici. È possibile che alcuni studi ad arruolamento attuale dei partecipanti (vedi punto 2.1.1.) prevedano anche la selezione di dati di ricerca dalle cartelle cliniche.

La selezione dalle cartelle cliniche è a cura del designato al trattamento cui lo studio si riferisce previa autorizzazione della direzione sanitaria dell'IRCCS. Il designato si avvarrà di autorizzati al trattamento della propria unità per la raccolta manuale dei dati dalle cartelle cliniche cartacee o di un designato/autorizzato dell'area IT nel caso di estrazione delle cartelle cliniche elettroniche.

2.1.3. Selezione dalla biobanca

Il servizio biobanca è dedicato alla conservazione dei campioni biologici raccolti dall'IRCCS per il loro futuro utilizzo in attività di ricerca medica, biomedica ed epidemiologica.

Nel caso in cui un progetto di studio preveda il trattamento di campioni biologici/dati genetici, l'unità di ricerca interessata può chiedere al servizio biobanca un'estrazione di campioni biologici/dati genetici utili alle finalità dello studio. In questo caso, il servizio biobanca provvede al ricontatto degli interessati al fine di proporre la partecipazione allo studio, come descritto al punto 2.1.1, fatte salve le eccezioni previste dall'art. 110 e 110bis comma 4 del codice privacy (come dettagliato in tabella al par. 3.1). Successivamente al ricevimento e alla valutazione della richiesta - come esplicitato nel Regolamento vigente per la Biobanca – e degli opportuni consensi specifici (anticipati sempre dall'invio di idoneo documento informativo ex art. 13 del GDPR), un autorizzato al trattamento del servizio biobanca provvede alla selezione, estrazione e comunicazione, ricevendo l'apposito supporto da SOL S.p.A. (fornitore del servizio di trasporto e stoccaggio di campioni biologici). Successivamente, il trattamento e la conservazione dei campioni biologici e dei relativi dati (inclusi eventuali dati genetici) ~~genetici~~ passano temporaneamente in capo all'unità di ricerca richiedente.

Alla biobanca sono dedicati spazi fisici ed informatici (database e cartelle di rete) autonomi, ai quali è garantito l'accesso solo al designato al trattamento del servizio e ai suoi autorizzati. Alla raccolta di un nuovo campione biologico viene generato un "codice biobanca", il quale verrà utilizzato al posto dei dati anagrafici dell'interessato (la gestione del codice e dei dati anagrafici avviene in maniera del tutto analoga alla modalità di gestione del documento di conversione descritta al punto 3.6.). Il campione biologico è quindi utilizzato per le attività progettuali previste e/o inviato e conservato presso la biobanca (a cura di SOL S.p.A).

La conservazione dei campioni biologici avviene dedicando ~~a questi~~ spazi e depositi idonei a garantirne, con misure di sicurezza tecniche ed organizzative, la qualità, l'integrità, la disponibilità, la tracciabilità e la sicurezza.

2.1.4. Ricevimento da altri centri di sperimentazione

I dati di ricerca possono provenire da altri centri nel caso l'IRCCS sia coordinatore della ricerca o di parti della stessa o nel caso altre strutture forniscano un servizio. I dati ricevuti sono sempre preventivamente pseudonimizzati tramite la sostituzione del nome e cognome con un codice alfanumerico in modo tale che solo il centro che li ha raccolti possa risalire all'interessato.

I dati di ricerca possono essere ricevuti via email con password di sicurezza (trasmessa con un canale di comunicazione differente), tramite sistemi di file sender (es. GARR) o con protocolli di trasferimento file (es. FTP). In alternativa, ricercatori individuali possono ricevere credenziali per l'accesso a portali realizzati da altri centri partecipanti.

2.2. Processo in caso di arruolamento del partecipante

2.2.1. Visita di screening

Il progetto inizia con l'invito del partecipante alla visita di screening; questo incontro ha la funzione di valutare il soddisfacimento dei criteri di inclusione/esclusione dello studio.

In considerazione dei criteri di inclusione/esclusione del singolo studio, la visita di screening può integrare un semplice colloquio o comprendere l'esecuzione di visite ed esami e la somministrazione di test (per esempio quando i criteri di inclusione si riferiscono a determinati punteggi del QI, particolari valori presenti nel sangue, ecc.).

È con il superamento (positivo) della visita di screening che il soggetto può procedere con il percorso di ricerca.

2.2.2 Visita/valutazione iniziale

Alla visita di screening segue la visita/valutazione inziale la quale, tipicamente, può prevedere: visita clinica, test in uso in neurologia e psichiatria e/o esami strumentali. Questa fase è necessaria per raccogliere i dati del partecipante prima che questo venga sottoposto all'intervento sperimentale.

2.2.3 Intervento sperimentale

L'intervento sperimentale, ovvero l'esecuzione della/e attività centrali nel progetto di studio al fine di poter raggiungere i risultati auspicati, prevede interventi farmacologici e/o non farmacologici, ad esempio riabilitazione cognitiva, neuromodulazione / neurostimolazione, psicoterapia, interventi di psico-educazione.

2.2.4 Valutazione intermedia, di fine trattamento e follow up

Durante e/o alla conclusione dell'intervento sperimentale vengono effettuate più valutazioni di tenore analogo alla visita/valutazione iniziale. Tipicamente sono una o più valutazioni intermedie, una visita di fine trattamento e una visita di follow up dopo un certo periodo determinato nel progetto di studio.

La funzione di questi passaggi è quella di raccogliere i dati del partecipante durante e/o dopo che questo è stato sottoposto all'intervento sperimentale e di monitorarne gli sviluppi ad intervalli definiti; in assenza di questi passaggi non si potrebbe osservare con la dovuta precisione il raggiungimento o meno dei risultati auspicati.

2.3. Casi particolari

Singoli progetti possono prevedere variazioni e/o modalità differenti di esecuzione dei vari passaggi e attività/passaggi addizionali.

2.3.1. Prelievo di materiale biologico

Il singolo progetto può richiedere un prelievo di materiale biologico, questo può avvenire per le seguenti ragioni:

- Deposito presso la biobanca per futuri progetti di ricerca (vedi punto 2.1.3.), previo ricontatto dell'interessato per autorizzarne l'utilizzo per lo specifico progetto; fatte salve le eccezioni previse dall'articolo 110 e 110bis comma 4 del Codice Privacy (come dettagliato in tabella al Par. 3.1)".Il progetto di studio prevede la raccolta di campioni biologici e relativi dati (inclusi eventualmente dati genetici).
- Il progetto di studio prevede una procedura opzionale di studio per la quale, previo rilascio di specifico consenso al trattamentoè prevista la raccolta di campioni biologici/dati genetici.

2.3.2. Incontri e visite a distanza

I passaggi descritti dal punto 2.2.1. al 2.2.4. sono generalmente organizzati in presenza. Questo non esclude che alcuni passaggi vengano eseguiti a distanza tramite teleconferenza, con tutte le precauzioni necessarie previste da un apposito addendum informativa per mantenere riservati i colloqui. Questo può avvenire:

- Per particolari esigenze di studio (es. protocollo di ricerca che valuta l'effetto della tele-riabilitazione);
- Per rispondere a situazioni/condizioni particolari (es. prevenzione dal contagio COVID-19).

2.3.3. Utilizzo di app

Alcuni specifici progetti di studio prevedono l'utilizzo di app. Quando queste sono fornite da terze parti, a seconda dei casi, queste ultime rivestono il ruolo di:

- Responsabili del trattamento: quando forniscono l'app ai centri partecipanti allo studio;
- Titolari del trattamento: quando è uno dei centri sperimentatori a fornire l'app.

Nel caso in cui un progetto di studio preveda l'utilizzo di app da parte della PLV (a prescindere che siano o meno fornite da terze parti), la stessa dovrà valutare la redazione di un apposito approfondimento al presente documento, anche utilizzando eventuali documentazioni (comprese valutazioni dei rischi o d'impatto sulla protezione dei dati) rese disponibili dal fornitore dell'app.

2.3.4. Progetti di rete

Sempre più spesso si presenta la possibilità/necessità per la PLV (tramite l'IRCCS) di prendere parte a progetti di rete, ovvero a progetti che possono anche prevedere la creazione di interconnessioni tra banche dati autonomamente create e amministrate al fine di rendere disponibili maggiori quantità di dati per fini di ricerca in determinati ambiti.

Tipicamente, ogni centro aderente al progetto di rete arruola i propri partecipanti, fornendo la propria informativa e curando di raccogliere il/i consenso/i al trattamento dei dati, preoccupandosi di informare gli interessati di tutti i dettagli relativi al particolare progetto. Le banche dati così generate sono interconnesse. Il risultato di questa interconnessione è la creazione di uno spazio differente dalle singole banche dati nel quale si possono trovare tutti i dati raccolti dai singoli partecipanti (a seconda dei casi, è ravvisabile una contitolarità del trattamento per la creazione di questi spazi e/o una nomina a Responsabile del trattamento laddove tale spazio sia affidato alla gestione/manutenzione di un soggetto terzo ai singoli centri di sperimentazione). Lo spirito che anima tali progetti è quello della massimizzazione del potenziale dei dati di ricerca e della condivisione di tali informazioni nell'interesse pubblico.

Nel caso in cui la PLV aderisca ad un progetto di rete dovrà essere valutata la redazione di un apposito approfondimento al presente documento.

2.3.5. Utilizzo di intelligenza artificiale (IA)

Alcuni progetti di studio potrebbero prevedere lo sviluppo e/o l'utilizzo di algoritmi di intelligenza artificiale (IA), sia di tipo classico che generativo, finalizzati all'analisi dei dati clinici e dei dati omici raccolti. Tali soluzioni, spesso incorporate in software dedicati e specificamente sviluppati per il singolo progetto, risultano destinate all'esecuzione di attività mirate di trattamento dei dati di ricerca, quali: estrazione, processamento e normalizzazione dei dati; elaborazione e classificazione di dataset clinici ed omici; raffronto e correlazione tra fonti eterogenee (es. dati clinici, genetici, ambientali, comportamentali); interconnessione e modellizzazione predittiva a fini diagnostici, terapeutici o esplorativi.

In considerazione della natura particolarmente sensibile dei dati trattati e dell'elevato rischio di effetti indiretti sui diritti e le libertà fondamentali degli interessati, la PLV dovrà valutare la redazione di un approfondimento specifico all'interno della struttura per mezzo di apposito regolamento interno. Tale approfondimento comprenderà:

1. Analisi etica dell'utilizzo dell'IA
   È opportuna valutazione dei rischi di bias algoritmico e di discriminazioni nei risultati, specie se basati su dataset clinici o genetici incompleti o non rappresentativi; la verifica del livello di trasparenza, spiegabilità e tracciabilità dei sistemi di IA adottati; ed infine una considerazione dei profili etici connessi alla natura dei dati omici (genomici, trascrittomici, proteomici, ecc.) e clinici, per i quali il rischio di re-identificazione è particolarmente elevato.

2. Adeguamento normativo
   - applicazione delle disposizioni del GDPR e delle linee guida dell'EDPB relative al trattamento di dati sanitari e genetici;
   - considerazione degli obblighi derivanti dall' AI Act, in particolare per i sistemi classificati come ad alto rischio nel settore sanitario e della ricerca;

- adozione di tecniche di pseudonimizzazione e anonimizzazione per ridurre il rischio di re-identificazione, specie in relazione ai dati omici.

3. Misure di mitigazione e sicurezza
   - implementazione di controlli di sicurezza informatica proporzionati alla sensibilità dei dati clinici ed omici;
   - definizione di metriche per monitorare qualità e rappresentatività dei dati di input;
   - predisposizione di piani di gestione degli incidenti e delle anomalie algoritmiche, con procedure di risposta rapide ed efficaci.
   - formazione specifica per utilizzo dell'IA.

L'adozione di tali misure garantirà che l'impiego di algoritmi di IA per l'elaborazione di dati clinici e omici avvenga nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione dei dati e accountability, rafforzando la solidità scientifica dei progetti di ricerca e la loro conformità etico-giuridica.

In questo caso la PLV dovrà valutare la redazione di un apposito approfondimento al presente documento, con relativa analisi etica dell'utilizzo di tali soluzioni.

2.4. Approfondimento sulle attività di trattamento eseguite nei vari processi

Per quanto riguarda i dettagli delle attività di trattamento eseguite nel singolo studio, laddove rilevanti, si rimanda a quanto indicato nel progetto di studio. La PLV è libera di valutare la redazione di un apposito approfondimento al presente documento laddove un singolo progetto di studio preveda particolari attività di trattamento tali da alterare, nella sostanza, le valutazioni riportate nella presente DPIA Generale.

3. Attività di trattamento di dati personali

Le attività descritte al paragrafo precedente comportano necessariamente il trattamento di dati personali; queste attività dovranno sempre essere svolte nel rispetto dei princìpi di seguito riportati.

3.1. Finalità e fondamenti di liceità del trattamento

Le finalità, e i rispettivi fondamenti di liceità, del trattamento perseguite dal Titolare in esecuzione delle attività oggetto del presente documento (e meglio descritte al paragrafo precedente) sono:

FINALITA'	FONDAMENTO DI LICEITA' E NORMATIVA DI RIFERIMENTO
1) Esecuzione del progetto di ricerca per il quale i dati sono stati raccolti.	Art. 6, comma 1, lett. a) e art. 9, comma 2, lett. a) del GDPR, ovverosia il consenso dell'interessato.
2) Ricontatto degli interessati al fine di proporre la partecipazione ad uno studio prospettico e/o interventistico.	Art. 6, comma 1, lett. a) e art. 9, comma 2, lett. a) del GDPR, ovverosia il consenso dell'interessato.
3) Ricontatto degli interessati (soggetto che non ha avuto accesso alla struttura per svolgere delle cure presso l'IRCCS ma è stato reclutato solo ai fini della ricerca) al fine di richiedere l'autorizzazione di questi al riutilizzo dei dati/campioni biologici in altri studi.	Art. 6, comma 1, lett. a) e art. 9, comma 2, lett. a) del GDPR, ovverosia il consenso dell'interessato. Ai sensi dell'art. 110 del Codice Privacy, quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca , il trattamento potrà essere effettuato anche in assenza di un consenso. In tali casi, è necessario dare evidenza scritta di tali impedimenti, debitamente comprovati, ed è necessario pubblicare l'informativa e la valutazione d'impatto sul sito internet dell'IRCCS.
4) Esecuzione di attività di ricerca scientifica sui dati raccolti durante l'erogazione delle prestazioni sanitarie.	. "Ai sensi dell'art 110bis comma 4 del Codice Privacy, i dati e i campioni biologici ~~raccolti~~ relativi a soggetti pervenuti in IRCCS per fini di cura potranno essere trattati anche per l'attività di ricerca a seguito del carattere strumentale che, negli IRCCS, l'attività clinica svolge nei confronti di quella scientifica. In tali casi, è necessario pubblicare l'informativa e la valutazione d'impatto sul sito internet dell'IRCCS

3.1.1. Valutazione dell'opportunità del trattamento considerate le finalità

Le attività analizzate dal presente documento sono tutte rientranti nel concetto di "attività di ricerca scientifica", con le relative peculiarità considerando il tipo di ricerca e le singole finalità del trattamento.

Ciò che la PLV vuole dimostrare in questo paragrafo è che, di fatto, le finalità del trattamento indicate al punto 3.1. sono riconosciute e condivise anche dalla collettività e, di conseguenza, dimostrare che l'attività di ricerca svolta con le caratteristiche e con le modalità descritte nel presente documento sia non solo opportuna, ma anche di vitale importanza.

Le attività degli IRCCS, come già detto, sono disciplinate dal d.lgs. 288/03, il quale, all'art. 1, riconosce il rilievo nazionale delle attività svolte da questi ("*Gli Istituti di ricovero e cura a carattere scientifico sono enti a rilevanza nazionale [..] che, secondo standards di eccellenza, perseguono finalità di ricerca, prevalentemente clinica e traslazionale, nel campo biomedico e in quello dell'organizzazione e gestione dei servizi sanitari ed effettuano prestazioni di ricovero e cura di alta specialità o svolgono altre attività aventi i caratteri di eccellenza di cui all'articolo 13, comma 3, lettera d)*") e continua, all'art. 13, comma 3, lettera d) facendo particolare focus sull'eccellenza dell'attività di ricerca svolta ("*caratteri di eccellenza del livello dell'attività di ricovero e cura di alta specialità direttamente svolta negli ultimi tre anni, ovvero del contributo tecnico-scientifico fornito, nell'ambito di un'attività di ricerca biometrica riconosciuta a livello nazionale e internazionale, al fine di assicurare una più alta qualità dell'attività assistenziale, attestata da strutture pubbliche del Servizio sanitario nazionale*").

Non a caso l'attività di ricerca medica retrospettiva sui dati clinici raccolti presso gli IRCCS trova apposita disciplina all'interno della normativa italiana in tema di protezione dei dati personali (art. 110bis, comma 4, d.lgs. 196/03). Tale previsione normativa, infatti, allenta la severità dell'ordinamento giuridico italiano in tema di ricerca medica, biomedica ed epidemiologica, accostando tale specifico settore a quanto generalmente previsto dal GDPR (l'attività di ricerca scientifica è essa stessa il fondamento di liceità per i trattamenti necessari a raggiungere tale finalità).

Risulta quindi riconosciuto (anche a livello normativo) che l'attività di ricerca eseguita dagli IRCCS sia un valore di massima rilevanza nazionale, il cui interesse preminente è quello di tutela della salute. La PLV, in questa analisi, intende per "tutela della salute", la ricerca di modalità atte a garantire il più elevato standard di salute fisica e mentale possibile per un individuo e/o per la collettività. La salute è un diritto fondamentale dell'essere umano, essendo elemento basilare della sua sopravvivenza, e, di conseguenza, è anche un interesse condiviso dalla collettività.

La PLV non rileva interessi contrapposti rispetto alle finalità del trattamento illustrate, ma, semmai, ulteriori interessi meritevoli di tutela, ovvero:

INTERESSE CONSIDERATO	SOLUZIONE ADOTTATA DALLA PLV
Rispetto del principio di liceità del trattamento.	Il rispetto da parte della PLV di questo principio è garantito da un'attenta analisi dei fondamenti di liceità dei trattamenti eseguiti per l'area ricerca, come risulta dalla redazione di questo documento e dalla diffusione degli estratti del Registro delle attività di trattamento del Titolare a tutti i designati al trattamento.

Rispetto dei principi di correttezza e trasparenza.	L'assoluta correttezza e trasparenza dei trattamenti effettuati è assicurata dalla menzione delle finalità del trattamento (e di tutti gli altri elementi richiesti dall'art. 13 del GDPR) nelle informative dedicate alle categorie di interessati ai trattamenti in analisi, delle quali i designati e gli autorizzati al trattamento gestiscono diligentemente la consegna (Procedura PR-PRY-001), e dalla consegna a tutti i partecipanti a progetti di ricerca di tutte le informazioni utili alla piena comprensione del progetto di studio.
Rispetto del principio di esattezza.	L'esattezza dei dati raccolti e delle valutazioni che ne derivano è assicurata, da una parte, dall'altissimo livello di professionalità di tutti i designati e autorizzati al trattamento e, dall'altra, dall'utilizzo di prassi, test, metodologie ecc. condivise e riconosciute dalla comunità scientifica.
Rispetto del principio di minimizzazione del dato.	La minimizzazione del dato è disciplinata da apposita procedura dedicata all'area ricerca dell'IRCCS (Procedura PR-PRY-004). Il designato al trattamento vigila sul pieno rispetto della procedura.
Rispetto del principio di limitazione della conservazione.	La PLV ha definito con chiarezza i tempi di conservazione dei dati personali riferendosi al Titolario e Massimario di scarto della Regione Lombardia (V.04/2018), documento redatto da un'amministrazione pubblica e dall'altissimo livello di dettaglio, nonché dalla normativa europea e nazionale in materia.
Rispetto dei principi di integrità e riservatezza.	Il rispetto di questi principi è dimostrato ai punti 4 e 5, come risultato dell'applicazione della Procedura PR-PRY-005.
La PLV, poi, assicura il rispetto di questi princìpi tramite la formazione generale e specifica in tema di protezione dei dati personali di tutto il personale coinvolto nelle attività di trattamento prese in esame dal presente documento. Il DPO della PLV, a seguito di un audit (26/10/2021) dedicato all'attività di ricerca, retrospettiva e prospettica, nonché alle sperimentazioni cliniche, compresi i casi in cui siano raccolti campioni biologici degli interessati, ha affermato che le diverse tipologie di ricerca e sperimentazioni attive presso l'IRCCS sono ben presidiate e gestite e che i trattamenti di dati personali derivanti risultano conformi alla normativa in vigore, rispettando i principi di: minimizzazione del dato, pseudonimizzazione e/o anonimizzazione dei dati, raccolta di liberi, specifici e distinti consensi nonché di informazione verso gli interessati.	

Considerato quanto sopra riportato, la PLV è sicura che le attività di trattamento così come progettate ed eseguite siano idonee a raggiungere le finalità sopra indicate nel pieno rispetto dei principi di cui all'art. 5 del GDPR.

3.2. Tempi di conservazione

La PLV ha identificato come riferimento generale per i tempi di conservazione dei dati personali trattati il Titolario e Massimario di scarto della Regione Lombardia (V.04/2018) nonché la normativa nazionale ed europea di settore. Per i trattamenti in oggetto, i dati verranno conservati:

DATI/DOCUMENTI	TEMPI DI CONSERVAZIONE
Dati e documenti che riguardano le sperimentazioni cliniche farmacologiche (proposte di sperimentazioni, pareri del Comitato Etico, sottoscrizioni dei protocolli di studio, autorizzazione sperimentazione, ecc.).	Fino alla conclusione del progetto e per i successivi 25 anni (art. 58 Reg. UE 536/2014).
Informative e consensi al trattamento dei dati personali.	Illimitato – 10 anni dalla revoca del consenso.
Dati personali/campioni biologici raccolti esclusivamente per uno specifico studio.	Fino alla conclusione del progetto e per i successivi 25 anni.
Dati e documenti inseriti nella cartella clinica.	Illimitato, così come stabilito dalla circolare del Min. Sanità n.900 del 1986.
Dati personali/campioni biologici raccolti per finalità di conservazione di questi per il loro futuro riutilizzo in altri studi ~~(previo ricontatto e consenso specifico).~~	Fino alla revoca del consenso.

Scaduti i termini per la conservazione sopra indicati, i dati verranno resi anonimi o distrutti.

3.3. Categorie di interessati – soggetti vulnerabili

I partecipanti alle attività di ricerca organizzate dalla PLV o a quelle alle quali la PLV partecipa, non possono essere ricondotti ad una categoria omogenea di soggetti. Elementi ricorrenti ma non necessariamente condivisi dalla totalità degli interessati sono:

- La presenza di una determinata patologia (neurodegenerativa o psichiatrica) e, eventualmente, la sottoposizione ad una particolare terapia farmacologica;
- Anzianità;
- Status di paziente;
- Caregiver;
- Volontari sani a rischio per patologie neurodegenerative o psichiatriche;
- Volontari sani.

Praticamente tutti i soggetti sopra indicati (ad esclusione dei Volontari sani) consentono di riportare l'interessato all'interno della categoria "soggetto vulnerabile". In effetti, la PLV ritiene che anche il sol fatto di essere arruolato in un progetto di ricerca costituisca elemento sufficiente per rientrare nella suddetta categoria. Pertanto, la totalità degli interessati alle attività di trattamento oggetto del presente documento può essere ricompresa nella categoria "soggetto vulnerabile".

3.4. Categorie di soggetti autorizzati al trattamento

La PLV ha adottato un modello organizzativo per la protezione dei dati personali (MODORG-PRY-001 Per la protezione dei dati personali PLV, di seguito "il modello") che definisce lo schema delle responsabilità interne alla sua organizzazione. Il modello è liberamente consultabile da parte di tutto il personale nella intranet aziendale ed è stato pubblicizzato dall'Ufficio Privacy via e-mail e tramite incontri di formazione.

Il setting organizzativo interno definito nel modello si divide su più livelli di responsabilità (di seguito si riporteranno esclusivamente i profili di responsabilità relativi ai trattamenti oggetto del presente documento):

RUOLO PRIVACY	RUOLI AZIENDALI	COMPITI E RESPONSABILITA'
Ufficio Privacy	il privacy officer della PLV.	• Eseguire le attività di compliance della PLV alla normativa in materia di protezione dei dati personali; • Fornire supporto in materia di protezione dei dati personali ai Referenti Privacy di struttura e ai Designati al trattamento; • Raccogliere, analizzare e dare riscontro alle richieste di esercizio dei diritti dell'interessato; • Partecipare all'intero processo di valutazione e gestione degli eventi di violazione dei dati personali.
Referente Privacy di struttura	Direttore dell'IRCCS.	• Fornisce, limitatamente alla propria struttura, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi comprese le disposizioni interne e le norme di autoregolazione in materia di protezione dei dati personali; • Rappresenta il punto di contatto tra la struttura e l'Ufficio Privacy centrale; • Predispone gli atti di nomina dei Responsabili del trattamento riferibili alla propria struttura; • Nomina i Designati al trattamento nella propria struttura.
Designato al trattamento	Ogni responsabile di laboratorio, di unità e di servizio di ricerca; Direttrice scientifica.	• Fornisce, limitatamente al proprio ufficio/unità/area, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi comprese le disposizioni interne e le norme di autoregolazione in materia di protezione dei dati personali; • Nomina gli autorizzati al trattamento nel proprio ufficio/unità/area.
Autorizzato al trattamento	Tutti i dipendenti afferenti ai vari laboratori, alle varie unità e ai vari servizi di ricerca; afferenti alla direzione scientifica.	• Fornisce, limitatamente alle attività di trattamento svolte in esecuzione delle proprie mansioni, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi comprese le disposizioni interne e le norme di autoregolazione in materia di protezione dei dati personali.

Ogni figura dello schema sopra riportato (escluso l'Ufficio Privacy) rispetta i propri compiti e le proprie responsabilità tramite le conoscenze acquisite durante la formazione in materia di protezione dei dati personali (sia generale che specifica per settore di attività) e con il supporto delle figure sovraordinate e dell'Ufficio Privacy.

3.5. Categorie di dati personali trattate – dati sensibili di natura estremamente personale

Ogni attività di ricerca comporta la necessità di raccogliere e trattare:

- Dati personali "comuni": dati anagrafici, codice attribuito al partecipante;
- Categorie particolari di dati inclusi i dati relativi alla salute: risultati di test e/o esami (comprese indagini strumentali come RM, PET, ECG, ecc.).

Alcuni progetti, poi, potrebbero necessitare la raccolta di alcune o di tutte le seguenti categorie di dati personali (a titolo non esaustivo):

- Dati personali "comuni":
  - Dati di contatto;
  - Informazioni sull'utilizzo di dispositivi, smartphone e app, comprese immagini, video e registrazioni audio;
  - Informazioni sullo stato famigliare e la sua composizione;
  - Altezza, peso e altre caratteristiche fisiche;
  - Titolo di studio, situazione lavorativa ed altre esperienze;
  - Abitudini alimentari e stile di vita;
  - Informazioni riguardanti episodi di vita presenti e passati, commissione di atti violenti;
  - Dati relativi alla posizione geografica, agli spostamenti e alla velocità di questi.
- Dati relativi alla salute:
  - Informazioni riguardo la presenza di malattie neurodegenerative o psichiatriche, patologie concomitanti, assunzione di determinati farmaci, assunzione di sostanze stupefacenti;
  - Informazioni acquisite dall'analisi dell'utilizzo di dispositivi e app, comprese immagini, video e registrazioni audio;
  - Informazioni relative al rimo sonno-veglia.

3.5.1. Dati genetici

Alcuni progetti prevedono anche la raccolta di campioni biologici (vedi punto 2.6.1.). I dati genetici che potrebbero essere raccolti sono (a titolo non esaustivo):

- Dati genetici indicativi di malattie neuro-degenerative quali la malattia di Alzheimer, la demenza frontotemporale, la demenza con corpi di Lewy (e.g. mutazioni patogenetiche note risultanti da analisi dell'acido desossiribonucleico - DNA, livelli proteici ridotti risultanti dall'analisi di fluidi biologici quali plasma, indicativi di mutazioni nulle in DNA);
- Dati genetici associati a suscettibilità o al contrario a protezione per le malattie neuro-degenerative, quali la malattia di Alzheimer, la demenza frontotemporale e la demenza con corpi di Lewy, o per patologie psichiatriche, quali la schizofrenia, il disturbo bipolare, la depressione maggiore, il disturbo borderline di personalità (e.g. polimorfismi nella sequenza di DNA, profili di metilazione del DNA, profili di espressione risultanti dall'analisi dell'acido ribonucleico, RNA);
- Dati genetici potenzialmente associati alla risposta alla terapia farmacologica e non in pazienti con disturbi neurocognitivi e psichici ~~pazienti psichiatrici~~ (e.g. polimorfismi nella sequenza di DNA, profili di metilazione del DNA, profili di espressione risultanti dall'analisi dell'acido ribonucleico, RNA).

La PLV si impegna al rispetto dell'Autorizzazione Generale al trattamento dei dati genetici dell'Autorità Garante per la protezione dei dati personali n. 8/2016.

3.6. Modalità di raccolta e conservazione dei dati

Le modalità di raccolta dei dati seguono le logiche indicate al punto 2.1.

Conservazione: i dati di ricerca sono conservati: in formato elettronico: in apposite cartelle di rete dedicate al singolo studio, al quale hanno accesso solo il designato al trattamento e gli autorizzati al trattamento dell'unità, laboratorio o servizio di ricerca specifico. Il nome e cognome e, se raccolto, il codice fiscale del partecipante sono raccolti separatamente in un altro documento (sempre interno alla cartella di rete, c.d. "documento di conversione"); al loro posto verrà sempre utilizzato un codice attribuito al singolo partecipante svincolato da alcun riferimento all'interessato (per questo motivo non sono ammessi, a titolo esemplificativo: iniziali del nome e cognome, data di nascita, codice di cartella clinica, riferimenti alla diagnosi, ecc.). Il documento di conversione è crittografato e la chiave di decrittazione è in possesso esclusivo del designato al trattamento e di un suo delegato. L'accesso al documento di conversione avviene esclusivamente quando sia effettivamente necessario procedere alla identificazione di un partecipante (per esempio per esigenze di aggiornamento/rettifica dei dati) e i log di accesso e modifica sono tracciati e monitorati; In formato cartaceo: tutti i moduli e la documentazione consegnata al partecipante al momento dell'arruolamento e, in alcuni progetti di studio, anche i dati di ricerca.

- Campioni biologici/dati genetici: se vengono raccolti campioni biologici/dati genetici, la loro gestione dipende dalla finalità della raccolta:
  - Deposito presso la biobanca per futuri progetti di ricerca: la gestione è in capo alla biobanca dell'IRCCS. I dati direttamente identificativi dell'interessato, in maniera del tutto simile alle modalità riportate sopra, vengono tenuti separati in un documento di conversione, al loro posto verrà utilizzato un codice biobanca (mentre il campione biologico viene affidato a SOL S.p.A., il documento di conversione rimane nell'esclusiva disponibilità del servizio biobanca dell'IRCCS);
  - Il progetto di studio o una procedura opzionale di studio ne prevede la raccolta: la gestione è in capo all'unità di ricerca cui lo studio si riferisce; in questo caso, al dato genetico vengono applicate le regole di conservazione valide per le altre categorie di dati personali.

3.7. Categorie di destinatari

Sebbene molte attività di ricerca siano condotte autonomamente dalla PLV, soprattutto sulla base di convenzioni con il Ministero della Salute o con altri enti pubblici o privati, l'IRCCS partecipa anche a molti progetti nei quali assume il ruolo di centro di sperimentazione e, per dinamiche descritte dai singoli progetti di studio, si trova a dover condividere dati (aggregati e non) con lo Sponsor e/o con gli altri centri. Esiste, poi, la possibilità che l'IRCCS debba avvalersi di strutture esterne (sanitarie o centri analisi) per l'esecuzione di specifiche analisi/test che non è in grado di svolgere presso le altre strutture della PLV. Di seguito si elencano le categorie di destinatari ai quali potrebbero essere inviati (o con i quali si potranno condividere) i dati personali dei partecipanti (quindi non aggregati/anonimi).

3.7.1. Titolari del trattamento autonomi

Questa è la categoria più variegata; tra i Titolari autonomi destinatari dei dati rientrano:

- Pubbliche amministrazioni e autorità di vigilanza legittimate a richiedere i dati (limitatamente ai dati richiesti necessari all'esecuzione delle loro attività);
- Sponsor e centri sperimentatori quando specificatamente previsto dal protocollo di ricerca (e limitatamente a quanto previsto dal protocollo di ricerca);
- Repository pubblici nei casi di pubblicazione dei raw data (si veda il punto 3.8.).

3.7.2. Contitolari del trattamento

Potrebbero venire identificate delle contitolarità per alcune attività del trattamento finalizzate all'esecuzione del progetto di ricerca, soprattutto in progetti di rete (vedi punto 2.3.4.) nei quali si prevede la creazione/alimentazione di database comuni di ricerca dedicati a specifiche patologie. In questi contesti, i trattamenti di raccolta e conservazione dei dati nel database comune potrebbero essere considerati oggetto di contitolarità. In questi contesti, la stipula di accordi e regolamenti ex art. 26 del GDPR sarà sempre monitorata dall' Ufficio Privacy/DPO in concerto con i referenti dei contitolari.

3.7.3. Responsabili del trattamento

La categoria dei responsabili del trattamento è riconducibile, fondamentalmente, alle seguenti categorie:

- Centri analisi e strutture sanitarie: quando risulta necessario procedere all'esecuzione di test/esami che non sia possibile eseguire presso le strutture della PLV, l'IRCCS si appoggia a soggetti esterni, sempre nominati Responsabili del trattamento ex art. 28 del GDPR;
- Enti partecipanti a progetti di ricerca: Per lo più in progetti di rete (vedi punto 2.3.4.), è possibile che si identifichi uno o più responsabili del trattamento, visto il carattere accessorio delle loro attività rispetto a quelle degli altri enti partecipanti;
- SOL S.p.A.: Come già detto, la biobanca dell'IRCCS è fisicamente gestita dalla società SOL S.p.A., nominata Responsabile del trattamento. Per il deposito dei campioni in biobanca, SOL si occupa anche del trasporto di questi.

3.7.4. Trasferimenti extra UE e garanzie

Le categorie di destinatari di cui ai punti precedenti non sempre hanno sede all'interno dell'Unione Europea. Quando un destinatario ha sede all'esterno dell'UE (per lo più negli Stati Uniti d'America), le garanzie adottate dalla PLV sono due:

- Dove sia possibile e compatibile con i fini del trasferimento, i dati vengono anonimizzati;
- Dove l'anonimizzazione non sia possibile o non sia compatibile con le finalità del trasferimento, la PLV e il ricevente i dati siglano apposite clausole tipo di protezione dei dati come rese disponibili dalla Commissione Europea (ex art. 46, comma 2, lett. c) del GDPR).

3.7.4.1. TIA – trasferimenti verso USA per finalità di ricerca

In questo paragrafo si intende riportare la valutazione eseguita dalla PLV in merito ai trasferimenti di dati personali negli Stati Uniti d'America per finalità connesse all'esecuzione di un progetto di ricerca (finalità 1 e 2). La valutazione riportata di seguito è stata impostata sul modello proposto dalla IAPP (*International Association of Privacy Professionals*) - EU SCC Transfer Impact Assessment (TIA) Version 1.01 (September 1st, 2021).

1. DESCRIZIONE DEI TRASFERIMENTI DA ANALIZZARE

Esportatore	Provincia Lombardo Veneta dell'Ordine Ospedaliero di San Giovanni di Dio – Fatebenefratelli
Stato nel quale ha sede l'esportatore	Italia
Importatore	Centro di sperimentazione o Sponsor del progetto di ricerca.
Stato nel quale ha sede l'importatore	Stati Uniti d'America.

Contesto e finalità del trasferimento	Il trasferimento ha sempre luogo all'interno della procedura di studio o a conclusione della stessa (principalmente nel caso in cui l'importatore è lo Sponsor) per finalità connesse a quelle indicate al punto 3.1. numeri 1 e 2.
Categorie di interessati	Vedi punto 3.3.
Categorie di dati personali oggetto del trasferimento	Vedi punto 3.5.
Tecnologie utilizzate per il trasferimento	Il trasferimento oggetto della presente valutazione avviene sottoforma di allegato crittografato ad una e-mail inviata al referente dell'importatore per il progetto di ricerca. La chiave di decrittazione verrà comunicata in un momento e con una modalità differente.
Misure di sicurezza tecniche adottate	Dati inviati in forma crittografata, per il trattamento e l'archiviazione dei dati presso l'importatore vengono specificate apposite misure di sicurezza nelle clausole tipo di protezione dei dati di volta in volta stipulate.
Misure di sicurezza organizzative adottate	Formazione in tema di protezione dei dati personali a tutto il personale, procedura per la minimizzazione dei dati trattati in ambito ricerca e protezione dei dati direttamente identificativi degli interessati (Procedura PR-PRY-004), invio a referente per lo specifico studio, per il trattamento e l'archiviazione dei dati presso l'importatore vengono specificate apposite misure di sicurezza nelle clausole tipo di protezione dei dati di volta in volta stipulate.
Ulteriori trasferimenti dei dati importati	Normalmente i trasferimenti avvengono, alternativamente 1) per permettere al singolo centro sperimentatore di eseguire le attività previste dal progetto di studio 2) per trasmettere i dati a conclusione dello studio allo Sponsor; quindi di norma non vi sono ulteriori trasferimenti. Se in singoli casi fosse necessario prevedere ulteriori trasferimenti questi saranno oggetto di apposita TIA.

2. DEFINIZIONE DEI PARAMETRI DELLA TIA

Data di analisi	Prendere in considerazione la data di approvazione dell'ultima versione disponibile del presente documento.

Periodo di trasferimento preso in analisi	5 anni dall'approvazione dell'ultima versione disponibile del presente documento.
Livello di rischio residuo di accesso legittimo non autorizzato ritenuto accettabile	Ai fini della presente valutazione, il livello di rischio ritenuto accettabile è < 5% di possibilità.
Giurisdizione oggetto della TIA	Stati Uniti d'America.
Leggi e altri atti normativi rilevanti prese in considerazione dalla presente TIA	Art. 702 FISA, EO-12333, PPD-28.

3. DESCRIZIONE DELLE SALVAGUARDIE ADOTTATE

Sarebbe possibile per l'esportatore, sotto un aspetto pratico, tecnologico ed economico, trasferire i dati personali oggetti di questa valutazione in un paese che si trova all'interno dell'UE o che è soggetto ad una decisione di adeguatezza?	I trasferimenti vengono effettuati proprio in ragione del soggetto che deve ricevere i dati personali (quindi il centro sperimentatore o lo Sponsor), quindi non è possibile.
I dati personali oggetto di questa valutazione sono trasferiti sotto una delle deroghe previste dall'art. 49 del GDPR?	No.
I dati personali sono trasmessi in chiaro?	No, il documento contente i dati è crittografato.
I dati personali sono accessibili in chiaro da parte dell'importatore?	Si, l'importatore riceve la chiave di decrittazione separatamente. L'importatore necessita di accedere ai dati per partecipare correttamente allo studio (centro sperimentatore) o in funzione del ruolo di Sponsor.
Il trasferimento è protetto da una garanzia prevista dalla normativa in materia di protezione dei dati personali (artt. 44 ss. GDPR)? è auspicabile il rispetto di tale garanzia all'interno della giurisdizione dell'importatore?	Si, come indicato al punto 3.7.4. (clausole tipo di protezione dei dati come rese disponibili dalla Commissione Europea ex art. 46, comma 2, lett. c) del GDPR). È certo che tale garanzia sia pienamente applicabile nella giurisdizione dell'importatore.

4. ANALISI DEL RISCHIO DI ACCESSO LEGITTIMO NON AUTORIZZATO NELLA GIURISDIZIONE DELL'IMPORTATORE

Analisi della probabilità che, durante il periodo considerato, le seguenti argomentazioni legali permettano di impedire ad autorità locali di imporre all'importatore l'accesso ai dati personali basandosi atti normativi sopra richiamati:

1) l'importatore non è un provider di servizi di comunicazione elettronica e, quindi, resta al di fuori dall'applicazione degli atti normativi sopra richiamati.	90% - Per tutti i trasferimenti presi in analisi, infatti, l'importatore rientrerà nelle seguenti categorie (Università, centro di ricerca, società farmaceutica).
2) l'importatore non ha il possesso, la custodia o il controllo sui dati personali in chiaro e, quindi, non è in grado di fornire questi a fronte di una richiesta di accesso fondata sugli atti normativi sopra richiamati.	0% - i dati sono disponibili in chiaro all'importatore per i motivi sopra riportati.
3) il trasferimento dei dati personali o il contenuto di tali dati è da considerare come una comunicazione a un soggetto statunitense, il quale non può venire sorvegliato intenzionalmente da un'autorità locale, ma tale sorveglianza potrebbe avvenire nel caso in esame. Tuttavia, non trattandosi l'importatore di un soggetto rientrante nell'area applicativa della normativa sopra citata, la richiesta di accesso ai dati sarebbe infondata.	90% - la normativa sopra citata, infatti, si applica ai provider di servizi di comunicazione elettronica e, anche se il trasferimento in analisi potrebbe rientrare nel concetto di "comunicazione elettronica", l'importatore fa sempre parte di categorie di soggetti diversi da quelli sottoposti all'obbligo di collaborazione con autorità locali.
4) eseguire un accesso legittimo non autorizzato violerebbe una normativa straniera in un modo non consentito dalla dottrina statunitense e, quindi, ciò impedisce un'eventuale richiesta di accesso ai dati.	0% - sebbene un accesso legittimo non consentito certamente andrebbe a ledere in parte il Regolamento UE 679/2016, la PLV non ha contezza di dottrina statunitense che non consenta simili richieste di accesso.
5) Sono presenti altri fondamenti legali all'interno dell'ordinamento giuridico statunitense che impediscono l'accesso legittimo non autorizzato nel caso in esame?	0% - la PLV non ha contezza di atti normativi interni agli Stati Uniti d'America che impediscano l'accesso legittimo non autorizzato.
L'importatore è contrattualmente vincolato a difendere i dati personali da un tentativo di accesso legittimo non autorizzato?	Si, nelle clausole tipo di protezione dei dati siglate ogni volta è presente tale vincolo ("Obblighi dell'importatore in caso di accesso da parte di autorità pubbliche").
Qual è la percentuale di probabilità che, durante il periodo preso in esame, i dati	1% - la PLV e i suoi importatori non hanno mai esperito il ricevimento di simili richieste.

siano oggetto di richiesta di accesso legittimo non autorizzato basato sugli atti normativi sopra richiamati, considerando l'esperienza passata?	
Qual è la percentuale di probabilità che, durante il periodo preso in esame, l'importatore sia tecnicamente capace di ottenere i dati in chiaro, senza il permesso dell'esportatore, come conseguenza di una richiesta legittima di accesso fondata sugli atti normativi sopra richiamati.	100% - l'importatore ha accesso ai dati in chiaro.
Sono state adottate misure idonee a monitorare la validità delle circostanze prese in analisi durante l'intero periodo considerato?	Si, l'Ufficio Privacy e il DPO monitorano periodicamente l'evoluzione degli atti normativi sopra richiamati.

5. CONCLUSIONI

Qual è la percentuale di probabilità che argomentazioni legali falliscano nel prevenire un accesso legittimo non autorizzato.	1% - due argomentazioni riportano una percentuale di efficacia del 90% (quindi: sottoposizione della prima argomentazione (90%) → in 90 casi su 100 ha efficacia. In 10 casi non ha efficacia, sottoposizione seconda argomentazione (90%) → in 9 casi su 10 ha efficacia = se si applicano entrambe le argomentazioni in 99 casi (90+9) su 100 queste saranno efficaci).
Considerando quanto detto nella presente TIA, il rischio residuo di accesso legittimo non autorizzato è accettabile?	Si – ai fini della presente valutazione, è accettabile il rischio < 5% (vedi punto 2.), quello indicato al passaggio precedente è dell'1%.
Considerando quanto detto nella presente TIA, il trasferimento è permesso?	I trasferimenti negli Stati Uniti d'America, con le caratteristiche e alle condizioni sopra descritte, sono **PERMESSI** dalla PLV.

3.7.5. Trasporto dei campioni biologici

Quando i campioni biologici devono essere trasferiti come conseguenza di una delle ipotesi elencate ai punti da 3.7.1. a 3.7.4., questi saranno sottoposti alle seguenti regole di trasporto:

- Il campione biologico è contenuto in apposito contenitore multistrato, specificamente indicato per il trasporto e la conservazione di quello specifico tipo di campione biologico, garantendo l'integrità e la qualità dello stesso;

- Il contenitore garantisce l'unicità e la provenienza del campione biologico al suo interno senza riportare dati personali dell'interessato sulla superficie;
- Il contenitore è munito di apposite soluzioni idonee a garantire la non alterazione del campione biologico al suo interno durante il trasporto;
- I contenitori sono trasportati da personale qualificato e su mezzi che garantiscano l'inaccessibilità fisica dei primi a soggetti non autorizzati.

3.8. Dati grezzi di ricerca ("raw data")

Sempre più spesso le convenzioni con il Ministero della Salute per l'esecuzione di progetti di ricerca e con altri soggetti pubblici e privati richiedono la pubblicazione dei raw data di ricerca su repository pubblici.

Per "raw data" si intende: *tutti i dati iniziali, senza manipolazione, rielaborazione o filtraggio, che costituiscono la base su cui vengono effettuate successive analisi, valutazioni, grafici e tabelle per un articolo scientifico o progetto. Esempi di raw data possono essere qualsiasi misura/segnale/parametro anatomico, funzionale, fisiologico, quantitativo e/o qualitativo, che possa essere acquisito direttamente dal soggetto/paziente per mezzo di opportuni strumenti e metodiche, nonché l'output di qualsiasi strumento dedicato all'analisi di materiale biologico*.

Per "repository pubblico" si intende: *archivio liberamente consultabile, curato e riconosciuto dalla comunità scientifica di riferimento*.

La motivazione alla base di tale pubblicazione risente dell'orientamento che l'Unione Europea sta adottando riguardo la ricerca scientifica, ovvero quello per il quale il dato di ricerca deve poter essere riutilizzato in ragione del preminente e vitale interesse pubblico all'esecuzione di ricerche in ambito medico, biomedico ed epidemiologico.

La PLV abbraccia totalmente tale orientamento, riconoscendo e comprendendo il preminente interesse pubblico sul quale esso si basa. Tale attività, però, non è di facile esecuzione nel quadro giuridico italiano in materia di protezione dei dati personali; infatti, se il GDPR lascia ampio spazio di manovra sia alla ricerca scientifica (sempre che sia condotta in sicurezza) che alle attività a cura di interessi pubblici rilevanti (art. 9, comma 2, lettere g) e j) del GDPR) individuando autonomi fondamenti di liceità per queste finalità del trattamento, il d.lgs. 196/03 (così come armonizzato alla normativa comunitaria), all'art. 110 indica come inscindibile fondamento di liceità per i trattamenti legati alla ricerca in ambito medico, biomedico ed epidemiologico il consenso dell'interessato. A nulla servono le deroghe introdotte dallo stesso articolo alla richiesta di consenso per finalità di pubblicazione dei raw data.

Il consenso non è da solo un fondamento di liceità idoneo a sostenere il trattamento di pubblicazione dei raw data su repository pubblici; questo, in ragione del fatto che la pubblicazione è richiesto che sia massiva e sistematica; due caratteristiche difficilmente compatibili unicamente con le caratteristiche del consenso ex art. 7 del GDPR, comma 4.

Da una parte abbiamo, quindi, il fondamento di liceità del consenso, dall'altra troviamo la necessità per l'IRCCS di procedere a questa pubblicazione, pena il mancato riconoscimento/restituzione dei finanziamenti previsti dalle convenzioni per la ricerca, con conseguente diminuzione sostanziale delle possibilità di eseguire nuove ricerche e partecipare, quindi, alla tutela della salute (vedi definizione data al punto 3.1.1.).

La soluzione individuata dalla PLV è la seguente: il trattamento di pubblicazione dei raw data non viene considerato come dotato di autonoma finalità del trattamento, ma rientra nelle attività facenti parte del flusso di trattamenti per finalità di ricerca scientifica in ambito medico, biomedico e epidemiologico di volta in volta attivato per un progetto (e sorretto dal consenso al trattamento dei dati per finalità di ricerca). Ogni informativa indicherà, quindi, nella sezione "destinatari" l'indicazione di questa attività. Per ridurre al minimo

i rischi del trattamento la PLV ha adottato un'apposita procedura (Procedura PR-PRY-004 – Adempimenti propedeutici alla pubblicazione dei raw data su repository pubblici) che indica il processo di gestione per la pubblicazione dei raw data su repository pubblici.

La PLV è cosciente che la soluzione ad oggi utilizzata non è che un virtuoso arrangiamento, stante la presenza di un vuoto normativo; per questo motivo, la PLV auspica di ricevere indicazioni più chiare da parte del legislatore nazionale riguardo il fondamento di liceità del trattamento della pubblicazione dei raw data su repository pubblici. La soluzione che la PLV attende è quella di un sostanziale accostamento della disciplina della pubblicazione dei raw data al tenore del Regolamento UE 679/2016, e, quindi, l'utilizzo dei fondamenti di liceità di cui all'art. 9, comma 2, lettere g) e j) (interesse pubblico rilevante e finalità di ricerca scientifica) e la definizione di elevati standard di sicurezza.

3.8.1. Adempimenti propedeutici alla pubblicazione dei raw data su repository pubblici

La procedura PR-PRY-004 indica due generi di attività:

1) Accorgimenti applicabili a tutti i trattamenti relativi alla ricerca scientifica: misure tecniche e organizzative di protezione dei dati direttamente identificativi dei partecipanti al singolo progetto di ricerca (cifratura, controllo delle chiavi di decrittazione, spazi di archiviazione predeterminati e ad accesso ristretto, raccolta dei file di log di accesso/modifica dei documenti di conversione) e misure organizzative idonee a garantire il rispetto del principio di minimizzazione dei dati trattati;
2) Accorgimenti ulteriori e specifici per la pubblicazione dei raw data: misure organizzative di generalizzazione di tutti i dati da pubblicare su repository pubblico con particolari focus su dati altamente identificativi e dati genetici, volte ad abbassare al minimo prospettabile il potenziale identificativo dei dati. Per la scelta del repository si prendono in considerazione il posizionamento all'interno dell'Unione Europea, compliance con il GDPR e elevati standard di sicurezza informatica.

3.9. Misure a garanzia dei diritti dell'interessato

Ogni progetto di ricerca dell'IRCCS non può iniziare senza un preventivo parere favorevole del Comitato Etico competente, ove previsto, un organismo indipendente che vigila sulla tutela del partecipante in senso più ampio di quello previsto dalla normativa sulla protezione dei dati personali.

L'IRCCS è accreditato "Joint Commission International", certificazione internazionale che garantisce elevanti standard di cura del paziente e nell'ambito della ricerca scientifica.

3.9.1. Attività di informazione ex art. 13 e 14 del GDPR

La consegna dell'informativa privacy è un'attività specificamente disciplinata da apposita procedura interna (Procedura PR-PRY-001), la quale indica le attività di trattamento previste in ogni documento informativo ex artt. 13 e 14 del GDPR, i ruoli coinvolti nella consegna dell'informativa e nell'archiviazione delle evidenze riguardanti la consegna ed il consenso al trattamento dei dati.

Ogni designato al trattamento ha ben chiaro i flussi di trattamenti sotto la sua responsabilità, dal momento che tutti questi hanno partecipato ad attività di formazione in materia di protezione dei dati personali (sia generale che specifica per area) e che a tutti questi sono stati consegnati appositi estratti per area di competenza del registro delle attività di trattamento del Titolare.

3.9.2. Esercizio dei diritti dell'interessato

Ogni interessato è reso edotto della sua libertà (esercitabile direttamente o per tramite di chi ne fa le veci) di esercitare tutti i diritti lui riconosciuti dalla normativa in materia di protezione dei dati personali (artt. 7 e

15-21 del GDPR). Per esercitare tali diritti l'interessato è informato della presenza della sezione "esercita i tuoi diritti privacy" all'interno della pagina "Privacy" presente nel footer del sito della PLV www.fatebenefratelli.it. In alternativa, visto il rapporto continuativo che spesso si instaura tra autorizzati e designati al trattamento e partecipanti a progetti di ricerca, si prevede la possibilità per questi ultimi di esercitare i propri diritti direttamente in fase di colloquio.

L'intero processo di gestione dell'esercizio dei diritti dell'interessato è oggetto di apposita procedura interna (Procedura PR-PRY-002), la quale assicura il tempestivo riscontro all'interessato (nel rispetto delle scadenze previste dall'art. 12 del GDPR), l'esauriente spiegazione quando il diritto esercitato non può vedersi riconosciuto e il pieno riconoscimento dei diritti esercitati tramite il coinvolgimento di tutte le risorse necessarie interne ed esterne alla PLV. L'interno processo è gestito direttamente dall'Ufficio Privacy.

3.9.3. Tutela della dignità e dell'informazione genetica

Le attività descritte al punto 2, ed in particolar modo le varie visite previste dai progetti di studio, sono eseguite nel pieno rispetto della dignità e riservatezza degli interessati. A tal fine, le visite saranno organizzate in modo da non diffondere informazioni sui partecipanti a soggetti non autorizzati al trattamento, attraverso l'adozione di idonee misure organizzative.

Qualora il progetto di studio prevedesse l'esecuzione di test genetici, i risultati degli stessi verranno consegnati all'interessato mediante l'esecuzione di apposita consulenza genetica in presenza di un'equipe multidisciplinare. L'organizzazione di tali incontri risponde alla necessità di informare gli interessati sul significato, i limiti, l'attendibilità e la specificità dei test eseguiti, nonché le implicazioni dei risultati degli stessi.

4. Analisi dei rischi inerenti ai trattamenti

Il processo di analisi e valutazione dei rischi privacy (a prescindere che sia o meno parte integrante di una valutazione d'impatto per la protezione dei dati) è disciplinato da apposita procedura interna (Procedura PR-PRY-005), la quale indica le modalità di calcolo del rischio, i livelli di rischio ritenuti accettabili ed elenca gli eventi che devono essere valutati, lasciando la libertà di considerarne anche altri tenendo conto del contesto e della natura del trattamento.

Le analisi sotto riportate si applicano ai contesti descritti al paragrafo 2, affidando eventuali ulteriori valutazioni ad un documento separato e riguardante uno specifico trattamento, che per contesto e/o natura merita ulteriori approfondimenti.

4.1. Modalità di calcolo del rischio

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).						

4.2. Valutazione di R relativo ad eventi generali

Al fine della presente analisi si intende per "evento generale" quell'accadimento capace di generare un rischio per i diritti e le libertà delle persone fisiche indipendentemente dal supporto fisico o informatico sul quale si trovano i dati personali.

CATEGORIA	EVENTO	VULNERABILITA'	CONSEGUENZA	I	P	R
GENERALE	Pandemia	Trasmissione dell'infezione tramite contatti diretti/indiretti con contagiati	Possibile rallentamento nel riscontro agli interessati per l'esercizio dei loro diritti / possibile abbassamento della vigilanza sugli archivi cartacei	Moderato	Possibile	Medio
	Trattamento svolto in assenza di informativa / consenso	Soggetti autorizzati non consegnano l'informativa o non raccolgono il consenso degli interessati	Trattamento illecito	Significativo	Possibile	Medio-alto
	Impedimento all'esercizio del controllo sui dati personali da parte dell'interessato	Mancato rispetto della procedura di riconoscimento dei diritti dell'interessato	Violazione dei diritti dell'interessato	Significativo	Possibile	Medio-alto
	Mancato rispetto del periodo di conservazione dei dati personali	Autorizzati al trattamento ignorano i tempi di conservazione / inefficace politica di cancellazione dei dati personali	Violazione dei principi alla base del trattamento	Moderato	Possibile	Medio

4.2.1. Valutazione di RR relativo ad eventi generali

EVENTO	VULNERABILITA'	M.S. ORGANIZZATIVE	M.S. TECNICHE	RR
Pandemia	Trasmissione dell'infezione tramite contatti diretti/indiretti con contagiati	Policy sicurezza anti-contagio	Controllo elettronico della temperatura e presenza/assenza mascherina all'entrata	Basso
Trattamento svolto in assenza di informativa / consenso	Soggetti autorizzati non consegnano l'informativa o non raccolgono il consenso degli interessati	Autorizzazione al trattamento dei dati per tutto il personale, formazione generale e specifica in tema protezione dati a tutto il personale, PR-PRY-001, supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	-	Basso
Impedimento all'esercizio del controllo sui dati personali da parte dell'interessato	Mancato rispetto della procedura di riconoscimento dei diritti dell'interessato	Autorizzazione al trattamento dei dati per tutto il personale, formazione generale e specifica in tema protezione dati a tutto il personale, PR-PRY-002, supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	-	Basso
Mancato rispetto del periodo di conservazione	Autorizzati al trattamento ignorano i tempi di conservazione / inefficace politica di	Autorizzazione al trattamento dei dati per tutto il personale, formazione generale e specifica in tema protezione dati a tutto il personale, supporto diretto	-	Basso

dei dati personali	cancellazione dei dati personali	dell'Ufficio Privacy con designati e autorizzati al trattamento		

4.3. Valutazione di R su supporti fisici

Al fine della presente valutazione, si intende per "supporto fisico": archivi, cartelle e documenti cartacei e campioni biologici.

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 / possibili eventi di angoscia o depressivi	Significativo	Improbabile	Medio
	Fenomeni atmosferici	Tromba d'aria, alluvione, nubifragio	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	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 / possibili eventi di angoscia o depressivi	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 / possibili eventi di angoscia o depressivi	Significativo	Improbabile	Medio
PROBLEMI ORGANIZZATIVI	Errore umano	Condivisione dei documenti con soggetti non autorizzati / mancato rispetto delle misure di sicurezza	Possibile perdita di riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	Significativo	Possibile	Medio-alto
	Accesso non autorizzato (colposo)	Soggetto non autorizzato accede colposamente ai dati	Possibile perdita di riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	Moderato	Possibile	Medio

4.3.1. Valutazione di RR su supporti fisici

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, 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, trasporto sicuro dei campioni biologici	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, 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, 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

4.4. Valutazione di R su supporti informatici

Al fine della presente valutazione, si intende per "supporto informatico": cartelle di rete, software, app, memorie rimovibili, caselle di posta elettronica, pc, tablet e altra strumentazione informatica, macchinari medicali, ecc.

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	Lieve	Possibile	Medio-basso
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 / possibile rallentamento nel riscontro agli interessati per l'esercizio dei loro diritti	Lieve	Possibile	Medio-basso
	Malware	Virus informatici di vario genere	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	Estremo	Possibile	Medio-alto
ATTI DELIBERATI	Intercettazione delle comunicazioni	Intercettazione "man in the middle"	Possibile perdita disponibilità, integrità e/o riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	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 / possibili eventi di angoscia o depressivi	Estremo	Possibile	Medio-alto
PROBLEMI ORGANIZZATIVI	Errore umano	Condivisione dei documenti con soggetti non autorizzati / mancato rispetto delle misure di sicurezza	Possibile perdita di riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	Significativo	Possibile	Medio-alto
	Accesso non autorizzato (colposo)	Soggetto non autorizzato accede colposamente ai dati	Possibile perdita di riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	Moderato	Possibile	Medio

4.4.1. Valutazione di RR su 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-004, regolamento sull'utilizzo della strumentazione informatica	-	Basso
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

4.5. Valutazione di R su biobanca

La presente valutazione è dedicata alle attività di trattamento dei dati personali presso la biobanca dell'IRCCS, gestita da SOL S.p.A. (Sala Criobiologica presso la filiale di Pavia, Viale Certosa n.2), come descritto ai punti 1.2, 2.1.3, 2.3.1 e 3.6.

Come spiegato ai punti precedenti, il servizio biobanca non copre la totalità dei trattamenti relativi ai campioni biologici/dati genetici, essendo questi ultimi trattati e conservati anche presso le varie unità di ricerca in ragione dei singoli progetti di studio (per le analisi di R per questi trattamenti ci si riferisca, a seconda dei casi, alle analisi di cui ai punti 4.3, 4.4 e 4.6).

L'analisi di seguito riportata si fonda, necessariamente, sulle informazioni fornite da SOL S.p.A.

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

4.5.1. Valutazione di RR su 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	Automazione delle richieste di consegna e ritiro di campioni biologici	Basso

		autorizzato; politiche e procedure di gestione degli incidenti di sicurezza, procedura gestione data breach		

4.6. Valutazione di R riguardo la pubblicazione dei raw data

CATEGORIA	EVENTO	VULNERABILITA'	CONSEGUENZA	I	P	R
SICUREZZA DELLA PUBBLICAZIONE	Caricamento dati "in chiaro"	Mancato rispetto regole di minimizzazione e generalizzazione	Possibile perdita riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	Estremo	Improbabile	Medio
	Misure di sicurezza del repository insufficienti	Mancato utilizzo della lista di repository sicuri resa disponibile dalla PLV	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni / possibili eventi di angoscia o depressivi	Estremo	Improbabile	Medio

4.6.1. Valutazione di RR riguardo la pubblicazione dei raw data

EVENTO	VULNERABILITA'	M.S. ORGANIZZATIVE	M.S. TECNICHE	RR
Caricamento dati "in chiaro"	Mancato rispetto regole di minimizzazione e generalizzazione	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-004	-	Basso
Misure di sicurezza del repository insufficienti	Mancato utilizzo della lista di repository sicuri resa disponibile dalla PLV	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-004	-	Basso

4.7 Valutazione di R riguardo all'uso dell'IA

CATEGORIA	EVENTO	VULNERABILITA'	CONSEGUENZA	I	P	R
SICUREZZA	Caricamento dati "in chiaro"	Mancato rispetto regole di minimizzazione, generalizzazione ed anonimizzazione	Possibile perdita riservatezza / possibili discriminazioni	Estremo	Probabile	Alto
	Diffusione dei dati caricati	Violazione normativa privacy, diritti e libertà degli interessati.	Possibile perdita di disponibilità, integrità e/o riservatezza / possibili discriminazioni	Estremo	Possibile	Medio-alto
PROBLEMA TECNICO	Generazione informazioni scorrette da parte di IA (i.e.: allucinazioni)	Mancato controllo di qualità di informazioni generate da IA	Possibili discriminazioni e/o errori metodologici	Lieve	Possibile	Medio-Basso

4.7.1 Valutazione di RR riguardo all'uso dell'IA

EVENTO	VULNERABILITA'	M.S. ORGANIZZATIVE	M.S. TECNICHE	RR
Caricamento dati "in chiaro"	Mancato rispetto regole di minimizzazione, generalizzazione ed anonimizzazione	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-004	-	Medio
Diffusione dei dati caricati	Violazione normativa privacy, diritti e libertà degli interessati	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-004	-	Medio
Generazione informazioni scorrette da parte di IA	Mancato controllo di qualità di informazioni generate	Formazione specifica sull'utilizzo dell'IA	-	Basso

5. Misure di sicurezza adottate

5.1. Analisi delle misure di sicurezza relative agli eventi generali

EVENTO	M.S.	DESCRIZIONE	ATTENUA	VALORI FINALI DI I & P
Pandemia	Policy sicurezza anti-contagio	È stata predisposta una policy che detta rigide regole di sicurezza anti-contagio	P	I: Moderato P: Raro

	Controllo elettronico della temperatura e presenza/assenza mascherina all'entrata	Presso le strutture, a tutti gli accessi, viene eseguito sistematicamente (anche per il tramite di rilevatori automatici) il controllo della temperatura e della presenza/assenza della mascherina	P	
	PR-PRY-002	È stata approvata e pubblicata apposita procedura per la gestione dell'esercizio dei diritti dell'interessato, la quale prevede un doppio canale di esercizio dei diritti dell'interessato (tramite raccomandata o e-mail), la definizione dei ruoli e dei soggetti coinvolti e una procedura d'urgenza che passa la gestione delle richieste degli interessati dall'Ufficio Privacy al DPO	I	
Trattamento svolto in assenza di informativa / consenso	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	I: Lieve P: Raro
	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	
	PR-PRY-001	È stata approvata e pubblicata apposita procedura che definisce il processo di gestione dell'informativa privacy e di raccolta del consenso; sono condivisi con l'intranet aziendale i modelli di informativa aggiornati e la loro pubblicazione è resa nota a tutti i soggetti coinvolti nel processo di gestione	P	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento	P/I	
Impedimento all'esercizio del controllo sui dati personali da parte dell'interessato	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	I: Lieve P: Raro
	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	
	PR-PRY-002	È stata approvata e pubblicata apposita procedura per la gestione dell'esercizio dei diritti dell'interessato, la quale prevede un doppio canale di esercizio dei diritti dell'interessato (tramite raccomandata o e-mail), la definizione dei ruoli e dei soggetti coinvolti e una procedura d'urgenza che passa la gestione delle richieste degli interessati dall'Ufficio Privacy al DPO	P	
	Supporto diretto dell'Ufficio Privacy con	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso	P/I	

	designati e autorizzati al trattamento	disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento		
Mancato rispetto del periodo di conservazione dei dati personali	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	I: Lieve P: Raro
	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento	P/I	

5.2. Analisi delle misure di sicurezza per i trattamenti effettuati su supporti fisici

EVENTO	M.S.	DESCRIZIONE	ATTENUA	VALORI FINALI DI I & P
Incendio	Controlli periodici sugli impianti elettrici	Periodicamente sono organizzati controlli sull'impianto elettrico	P	I: Lieve P: Raro
	Estintori	Sono presenti e mappati estintori in tutti gli edifici, la loro presenza e conformità viene monitorata periodicamente	I	
	Presenza team anti incendio	Un team organizzato e previsto in apposita procedura è sempre pronto all'intervento. Il team ha frequentato il corso per la gestione degli incendi.	I	
	Documenti chiusi in armadi	Tutti gli archivi cartacei contenenti dati personali sono contenuti in armadi di vari materiali	I	
	Messa a terra	È presente la messa a terra di tutte le prese	P	
	Rilevatore di fumo	Sono presenti rilevatori di fumo in tutti gli uffici ed il loro funzionamento viene monitorato periodicamente	I	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
Allagamento	Controlli periodici sugli impianti idraulici	Periodicamente sono organizzati controlli sull'impianto idraulico	P	I: Lieve P: Raro
	Documenti chiusi in armadi	Tutti gli archivi cartacei contenenti dati personali sono contenuti in armadi di vari materiali	I	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per	I	

		un'efficace identificazione di tali eventi e la previsione di misure correttive		
Fenomeni sismici	Documenti chiusi in armadi	Tutti gli archivi cartacei contenenti dati personali sono contenuti in armadi di vari materiali	I	I: Lieve P: Raro
	Edifici antisismici	Tutti gli edifici sono stati eretti in osservanza della normativa edilizia in materia di edifici antisismici	P	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
Fenomeni atmosferici	Documenti chiusi in armadi	Tutti gli archivi cartacei contenenti dati personali sono contenuti in armadi di vari materiali	I	I: Lieve P: Raro
	Monitoraggio infissi	L'ufficio tecnico locale interviene tempestivamente per risolvere segnalazioni relative ad infissi difettosi o danneggiati	P	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
Deterioramento	Documenti chiusi in armadi	Tutti gli archivi cartacei contenenti dati personali sono contenuti in armadi di vari materiali	P	I: Minimo P: Raro
	Uffici climatizzati	Tutti gli uffici hanno un climatizzatore che imposta la temperatura ad un livello prefissato dalla struttura	P	
	Monitoraggio infissi	L'ufficio tecnico locale interviene tempestivamente per risolvere segnalazioni relative ad infissi difettosi o danneggiati	P	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
Accesso non autorizzato (doloso)	Documenti chiusi in armadi	Tutti gli archivi cartacei contenenti dati personali sono contenuti in armadi di vari materiali	P	I: Moderato P: Raro
	Uffici chiusi a chiave	Ogni ufficio, quando non presidiato, viene chiuso a chiave. Le chiavi di accesso agli uffici sono in possesso esclusivo di personale specificamente individuato ed esiste un registro per la consegna di queste	P	
	Controllo degli accessi alle strutture	Presso la struttura è presente una portineria che monitora h24 tutti gli accessi; inoltre, l'accesso all'area ricerca è riservato a soggetti autorizzati	P	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	

	Videosorveglianza	Presso la struttura sono presenti diversi impianti di videosorveglianza funzionanti h24	P	
	Allarme	Fuori dagli orari d'ufficio è attivo un sistema di allarme anti intrusione	I	
Intercettazione delle comunicazioni	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	I: Lieve P: Raro
	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	
	Nomine a Responsabile del trattamento per tutti i fornitori	Tutti i fornitori che trattano dati per conto della PLV sono nominati responsabili del trattamento con apposito atto che indica responsabilità e misure di sicurezza da adottare durante le attività di trattamento	P	
	Supporti cartacei trasmessi esclusivamente in busta chiusa all'interessato/delegato/soggetto autorizzato al trattamento/trasportatore esterno identificato e autorizzato	Ogni supporto cartaceo contenente dati dei partecipanti viene sempre consegnato in busta chiusa a soggetti legittimati a ritirare tali dati	P	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	Trasporto sicuro dei campioni biologici	I campioni biologici vengono trasportati sempre con mezzi che garantiscono la qualità, l'integrità, la disponibilità e la tracciabilità	P/I	
	Videosorveglianza	Presso la struttura sono presenti diversi impianti di videosorveglianza funzionanti h24	P	
Errore umano	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	I: Lieve P: Raro
	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento	P	

Accesso non autorizzato (colposo)	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	I: Minimo P: Raro
	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	
	Documenti chiusi in armadi	Tutti gli archivi cartacei contenenti dati personali sono contenuti in armadi di vari materiali	P	
	Documenti organizzati in archivi tematici	Tutti gli archivi cartacei sono organizzati in maniera ben definita	P	
	Uffici chiusi a chiave	Ogni ufficio, quando non presidiato, viene chiuso a chiave. Le chiavi di accesso agli uffici sono in possesso esclusivo di personale specificamente individuato ed esiste un registro per la consegna di queste	P	

5.3. Analisi delle misure di sicurezza per i trattamenti effettuati su supporti informatici

EVENTI	M.S.	DESCRIZIONE	ATTENUA	VALORI FINALI DI I & P
Incendio	Controlli periodici sugli impianti elettrici	Periodicamente sono organizzati controlli sull'impianto elettrico	P	I: Lieve P: Raro
	Estintori	Sono presenti e mappati estintori in tutti gli edifici, la loro presenza e conformità viene monitorata periodicamente	I	
	Presenza team anti incendio	Un team organizzato e previsto in apposita procedura è sempre pronto all'intervento. Il team ha frequentato il corso per la gestione degli incendi	I	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	Disaster recovery plan	È stato predisposto e condiviso un disaster recovery plan dedicato alla struttura, il quale indica ruoli, tempistiche e priorità d'intervento	I	
	Messa a terra	È presente la messa a terra di tutte le prese	P	
	Rilevatore di fumo	Sono presenti rilevatori di fumo in tutti gli uffici ed il loro funzionamento viene monitorato periodicamente	I	
	Controllo della temperatura nella sala server	La sala server è mantenuta ad una temperatura interna stabilita dai protocolli di sicurezza	P	

	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Allagamento	Controlli periodici sugli impianti idraulici	Periodicamente sono organizzati controlli sull'impianto idraulico	P	I: Lieve P: Raro
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	Disaster recovery plan	È stato predisposto e condiviso un disaster recovery plan dedicato alla struttura, il quale indica ruoli, tempistiche e priorità d'intervento	I	
	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Fenomeni sismici	Edifici antisismici	Tutti gli edifici sono stati eretti in osservanza della normativa edilizia in materia di edifici antisismici	P	I: Lieve P: Raro
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	Disaster recovery plan	È stato predisposto e condiviso un disaster recovery plan dedicato alla struttura, il quale indica ruoli, tempistiche e priorità d'intervento	I	
	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Fenomeni atmosferici	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	I: Lieve P: Raro
	Disaster recovery plan	È stato predisposto e condiviso un disaster recovery plan dedicato alla struttura, il quale indica ruoli, tempistiche e priorità d'intervento	I	
	Monitoraggio infissi	L'ufficio tecnico locale interviene tempestivamente per risolvere segnalazioni relative ad infissi difettosi o danneggiati	P	
	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Deterioramento	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	I: Lieve P: Raro
	Disaster recovery plan	È stato predisposto e condiviso un disaster recovery plan dedicato alla struttura, il quale indica ruoli, tempistiche e priorità d'intervento	I	
	Monitoraggio infissi	L'ufficio tecnico locale interviene tempestivamente per risolvere segnalazioni relative ad infissi difettosi o danneggiati	P	

	Controllo della temperatura nella sala server	La sala server è mantenuta ad una temperatura interna stabilita dai protocolli di sicurezza	P	
	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Indisponibilità infrastruttura	Disaster recovery plan	È stato predisposto e condiviso un disaster recovery plan dedicato alla struttura, il quale indica ruoli, tempistiche e priorità d'intervento	I	I: Lieve P: Raro
	Fornitori servizi ICT tempestivamente coinvolti	Tutti i fornitori di servizi ICT garantiscono un punto di contatto attivo h24 per supporto e interventi tempestivi	I	
	Gruppo di continuità (2 ore)	Tutte le sale server della struttura sono munite di un gruppo di continuità comune che garantisce un'autonomina di circa due ore	I	
	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Bug	Fornitori servizi ICT tempestivamente coinvolti	Tutti i fornitori di servizi ICT garantiscono un punto di contatto attivo h24 per supporto e interventi tempestivi	I	I: Minimo P: Possibile
Malware	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	I: Moderato P: Raro
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	PR-PRY-004	È stata approvata e pubblicata apposita procedura che definisce e impone standard di sicurezza informatica dei dati utilizzati per finalità di ricerca: separazione logica, raccolta dei log accesso/modifica, limitazione degli accessi logici, crittografia e controllo delle chiavi di decrittazione dei documenti di conversione (contenenti i dati direttamente identificativi dei partecipanti); misure organizzative a garanzia del rispetto del principio di minimizzazione dei dati trattati	P/I	
	Disaster recovery plan	È stato predisposto e condiviso un disaster recovery plan dedicato alla struttura, il quale indica ruoli, tempistiche e priorità d'intervento in caso di incidenti	I	
	Regolamento sull'utilizzo della strumentazione informatica	È stato approvato, pubblicato e consegnato a tutti i dipendenti un regolamento sull'utilizzo della strumentazione informatica, il quale regola, tra le altre cose: livelli minimi di sicurezza delle password e gestione delle stesse; modalità di utilizzo di software, cartelle di rete e navigazione Internet; controllo navigazione Internet da parte degli amministratori di sistema	P	

	Firewall	Su ogni dispositivo è presente un Firewall software (UFW)	P	
	Antivirus	Ogni dispositivo che entra nella rete aziendale dev'essere munito di software antivirus; tutti i PC aziendali sono muniti di software Sophos, i dispositivi non aziendali sono valutati caso per caso	P/I	
	File ban	Nella rete dedicata alla ricerca è presente un file ban, che banna gli attacchi ssh provenienti da fonti riconosciute come pericolose	P	
	Content filtering	La navigazione interna è contingentata da regole che prevedono il blocco di navigazione verso particolari siti considerati pericolosi o delicati	P	
	Sandbox	È presente un sandbox per tutte le caselle e-mail aziendali, che filtra e testa le comunicazioni in entrata	P	
	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Intercettazione delle comunicazioni	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	I: Lieve P: Raro
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	PR-PRY-004	È stata approvata e pubblicata apposita procedura che definisce e impone standard di sicurezza informatica dei dati utilizzati per finalità di ricerca: separazione logica, raccolta dei log accesso/modifica, limitazione degli accessi logici, crittografia e controllo delle chiavi di decrittazione dei documenti di conversione (contenenti i dati direttamente identificativi dei partecipanti); misure organizzative a garanzia del rispetto del principio di minimizzazione dei dati trattati	P/I	
	crittografia in transito	Il trasferimento dei dati avviene sottoforma di allegato crittografato ad una e-mail. La chiave di decrittazione viene comunicata in un momento e con una modalità differente	I	
Accesso non autorizzato (doloso)	Controllo degli accessi alle strutture	Presso la struttura è presente una portineria che monitora h24 tutti gli accessi; inoltre, l'accesso all'area ricerca è riservato a soggetti autorizzati	P	I: Lieve P: Raro
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	PR-PRY-004	È stata approvata e pubblicata apposita procedura che definisce e impone standard di sicurezza informatica dei dati utilizzati per finalità	P/I	

		di ricerca: separazione logica, raccolta dei log accesso/modifica, limitazione degli accessi logici, crittografia e controllo delle chiavi di decrittazione dei documenti di conversione (contenenti i dati direttamente identificativi dei partecipanti); misure organizzative a garanzia del rispetto del principio di minimizzazione dei dati trattati		
	Uffici chiusi a chiave	Ogni ufficio, quando non presidiato, viene chiuso a chiave. Le chiavi di accesso agli uffici sono in possesso esclusivo di personale specificamente individuato ed esiste un registro per la consegna di queste	P	
	Regolamento sull'utilizzo della strumentazione informatica	È stato approvato, pubblicato e consegnato a tutti i dipendenti un regolamento sull'utilizzo della strumentazione informatica, il quale regola, tra le altre cose: livelli minimi di sicurezza delle password e gestione delle stesse; modalità di utilizzo di software, cartelle di rete e navigazione Internet; controllo navigazione Internet da parte degli amministratori di sistema	P	
	Switch fisico dedicato alla ricerca	La rete aziendale e quella dedicata alla ricerca sono tenute separate e distinte; in ciascun rack si attesta uno switch fisico (o uno stack di switch fisici) dedicato	P	
	Cambio delle porte di connessione	Per la rete dedicata alla ricerca è regolato il cambio delle porte di connessione	P	
	Blocco di porte non strettamente necessarie	Le porte di connessione non necessarie vengono bloccate	P	
	Firewall	Su ogni dispositivo è presente un Firewall software (UFW)	P	
	Antivirus	Ogni dispositivo che entra nella rete aziendale dev'essere munito di software antivirus; tutti i PC aziendali sono muniti di software Sophos, i dispositivi non aziendali sono valutati caso per caso	P/I	
	Videosorveglianza	Presso la struttura sono presenti diversi impianti di videosorveglianza funzionanti h24	P	
	Allarme	Fuori dagli orari d'ufficio è attivo un sistema di allarme anti intrusione	P	
	Backup giornaliero (copertura 7 gg)	È eseguito il backup dei dati sul server a cadenza giornaliera	I	
Errore umano	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	I: Lieve P: Raro
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso	P	

		disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento		
	PR-PRY-003	È stata approvata e pubblicata apposita procedura per la gestione del data breach, la quale indica con chiarezza ruoli e passaggi per un'efficace identificazione di tali eventi e la previsione di misure correttive	I	
	PR-PRY-004	È stata approvata e pubblicata apposita procedura che definisce e impone standard di sicurezza informatica dei dati utilizzati per finalità di ricerca: separazione logica, raccolta dei log accesso/modifica, limitazione degli accessi logici, crittografia e controllo delle chiavi di decrittazione dei documenti di conversione (contenenti i dati direttamente identificativi dei partecipanti); misure organizzative a garanzia del rispetto del principio di minimizzazione dei dati trattati	P/I	
	Regolamento sull'utilizzo della strumentazione informatica	È stato approvato, pubblicato e consegnato a tutti i dipendenti un regolamento sull'utilizzo della strumentazione informatica, il quale regola, tra le altre cose: livelli minimi di sicurezza delle password e gestione delle stesse; modalità di utilizzo di software, cartelle di rete e navigazione Internet; controllo navigazione Internet da parte degli amministratori di sistema	P	
Accesso non autorizzato (colposo)	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	I: Lieve P: Raro
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	PR-PRY-004	È stata approvata e pubblicata apposita procedura che definisce e impone standard di sicurezza informatica dei dati utilizzati per finalità di ricerca: separazione logica, raccolta dei log accesso/modifica, limitazione degli accessi logici, crittografia e controllo delle chiavi di decrittazione dei documenti di conversione (contenenti i dati direttamente identificativi dei partecipanti); misure organizzative a garanzia del rispetto del principio di minimizzazione dei dati trattati	P/I	
	Regolamento sull'utilizzo della strumentazione informatica	È stato approvato, pubblicato e consegnato a tutti i dipendenti un regolamento sull'utilizzo della strumentazione informatica, il quale regola, tra le altre cose: livelli minimi di sicurezza delle password e gestione delle stesse; modalità di utilizzo di software, cartelle di rete e navigazione Internet; controllo navigazione Internet da parte degli amministratori di sistema	P	

5.4. Analisi delle misure di sicurezza adottate per la biobanca

EVENTI	M.S.	DESCRIZIONE	ATTENUA	VALORI FINALI DI I & P
Incendio	Impianti elettrici realizzati a regola d'arte	-	P	I: Moderato

	Estintori a polvere	Sono presenti e mappati estintori in tutti gli edifici, la loro presenza e conformità viene monitorata periodicamente	I	P: Raro
	Presenza team anti incendio	Un team organizzato e previsto in apposita procedura è sempre pronto all'intervento. Il team ha frequentato il corso per la gestione degli incendi	I	
	Istruzioni in caso di perdite di campioni biologici	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di perdite di campioni biologici	I	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Messa a terra	È presente la messa a terra di tutte le prese	P	
	Rilevatore di fumo	Sono presenti rilevatori di fumo ed il loro funzionamento viene monitorato periodicamente	I	
	Controllo della temperatura	La sala criobiologica è mantenuta ad una temperatura interna stabilita dai protocolli di sicurezza	P	
Allagamento	Controlli periodici sugli impianti idraulici	Periodicamente sono organizzati controlli sull'impianto idraulico	P	I: Moderato P: Raro
	Istruzioni in caso di perdite di campioni biologici	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di perdite di campioni biologici	I	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Monitoraggio umidità	Il tasso di umidità è monitorato e controllato nella sala criobiologica	P	
Fenomeni sismici	Campioni biologici conservate in aree fisicamente protette	Le aree dedicate a sala criobiologica sono situate in edifici solidi e protetti	P	I: Moderato P: Raro
	Istruzioni in caso di perdite di campioni biologici	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di perdite di campioni biologici	I	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
Fenomeni atmosferici	Campioni biologici conservate in aree fisicamente protette	Le aree dedicate a sala criobiologica sono situate in edifici solidi e protetti	P	I: Moderato P: Raro

	Istruzioni in caso di perdite di campioni biologici	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di perdite di campioni biologici	I	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Monitoraggio umidità	Il tasso di umidità è monitorato e controllato nella sala criobiologica	P	
Deterioramento	Campioni biologici conservate in aree fisicamente protette	Le aree dedicate a sala criobiologica sono situate in edifici solidi e protetti	P	I: Moderato P: Raro
	Istruzioni in caso di perdite di campioni biologici	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di perdite di campioni biologici	I	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Controlli anti-parassitari/derattizzazione	Sono eseguiti periodicamente controlli per evitare la presenza di parassiti/ratti	P	
	Servizio di pulizia	I locali sono mantenuti puliti e privi di accumuli di polvere	P	
	Controllo temperatura	La sala criobiologica è mantenuta ad una temperatura interna stabilita dai protocolli di sicurezza	P	
	Monitoraggio umidità	Il tasso di umidità è monitorato e controllato nella sala criobiologica	P	
	Monitoraggio atmosfera interna	L'atmosfera interna alla sala criobiologica è controllata e monitorata	P	
	Sistema di areazione	Nella sala criobiologica è presente un sistema di areazione	P	
Indisponibilità infrastruttura	Impianti elettrici realizzati a regola d'arte	-	P	I: Moderato P: Raro
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Gruppi di continuità	Sono presenti soluzioni di continuità energetica in caso di guasti, cali di tensione e simili	I	
Intercettazione delle comunicazioni	Autorizzazione al trattamento e formazione di tutti i dipendenti	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali e formato in materia di protezione dei dati personali	P/I	I: Moderato P: Raro

	Trasporto sicuro dei campioni biologici tramite contenitori e mezzi che assicurino la disponibilità, l'integrità, la provenienza e l'inalterabilità dei campioni biologici e la riservatezza dell'interessato	-	P/I	
	SOL S.p.A. non è in possesso delle anagrafiche deli interessati	Solo S.p.A. tratta esclusivamente i codici biobanca e non le anagrafiche degli interessati, riducendo la possibilità che questi vengano identificati	I	
	Non vengono utilizzati trasportatori terzi	Il non utilizzo di trasportatori terzi assicura un maggiore controllo sugli standard di sicurezza imposti	P	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Automazione delle richieste di consegna e ritiro di campioni biologici	Il sistema di richiesta di consegna e ritiro di campioni biologici è supportato da apposito software, il quale assicura l'identità del richiedente e diminuisce la possibilità di errori e fraintendimenti	P	
Accesso non autorizzato (doloso)	Autorizzazione al trattamento e formazione di tutti i dipendenti	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali e formato in materia di protezione dei dati personali	P/I	I: Moderato P: Raro
	Controllo accessi biometrico	L'accesso agli edifici è consentito solo previa identificazione biometrica	P	
	Accesso riservato al solo personale previamente autorizzato	L'accesso è riservato al personale previamente autorizzato ed indentificato, esclusivamente per ragioni di servizio	P	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Videosorveglianza h24 7 giorni su 7	Presso la struttura sono presenti diversi impianti di videosorveglianza funzionanti tutti i giorni h24	P	
Errore umano	Autorizzazione al trattamento e formazione di tutti i dipendenti	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali e formato in materia di protezione dei dati personali	P/I	I: Moderato P: Raro
	Trasporto sicuro dei campioni biologici tramite contenitori e mezzi che assicurino la disponibilità, l'integrità, la provenienza e l'inalterabilità dei campioni	-	P/I	

	biologici e la riservatezza dell'interessato			
	SOL S.p.A. non è in possesso delle anagrafiche deli interessati	Solo S.p.A. tratta esclusivamente i codici biobanca e non le anagrafiche degli interessati, riducendo la possibilità che questi vengano identificati	I	
	Non vengono utilizzati trasportatori terzi	Il non utilizzo di trasportatori terzi assicura un maggiore controllo sugli standard di sicurezza imposti	P	
	Politiche e procedure di gestione degli incidenti di sicurezza	Ogni dipendente ha ricevuto istruzioni chiare sulla gestione di incidenti di sicurezza	I	
	Procedura gestione data breach	È stata redatta e condivisa una procedura per la gestione degli eventi di violazione dei dati personali	I	
	Automazione delle richieste di consegna e ritiro di campioni biologici	Il sistema di richiesta di consegna e ritiro di campioni biologici è supportato da apposito software, il quale assicura l'identità del richiedente e diminuisce la possibilità di errori e fraintendimenti	P	
	Controllo accessi biometrico	L'accesso agli edifici è consentito solo previa identificazione biometrica	P	
	Accesso riservato al solo personale previamente autorizzato	L'accesso è riservato al personale previamente autorizzato ed indentificato, esclusivamente per ragioni di servizio	P	

5.5. Analisi delle misure di sicurezza adottate per la pubblicazione dei raw data

EVENTI	M.S.	DESCRIZIONE	ATTENUA	VALORI FINALI DI I & P
Mancato rispetto regole di minimizzazione e generalizzazione	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	I: Moderato P: Raro
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento	P	
	PR-PRY-004	È stata approvata e pubblicata apposita procedura che definisce e impone standard di sicurezza informatica dei dati utilizzati per finalità di ricerca: separazione logica, raccolta dei log accesso/modifica, limitazione degli accessi logici, crittografia e controllo delle chiavi di decrittazione dei documenti di conversione (contenenti i dati	P/I	

		direttamente identificativi dei partecipanti); misure organizzative a garanzia del rispetto del principio di minimizzazione dei dati trattati		
Mancato utilizzo della lista di repository sicuri resa disponibile dalla PLV	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P/I	I: Moderato P: Raro
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento	P	
	PR-PRY-004	È stata approvata e pubblicata apposita procedura che definisce e impone standard di sicurezza informatica dei dati utilizzati per finalità di ricerca: separazione logica, raccolta dei log accesso/modifica, limitazione degli accessi logici, crittografia e controllo delle chiavi di decrittazione dei documenti di conversione (contenenti i dati direttamente identificativi dei partecipanti); misure organizzative a garanzia del rispetto del principio di minimizzazione dei dati trattati	P/I	

5.6 Analisi Misure di sicurezza adottate nell'uso dell'IA

EVENTI	M.S.	DESCRIZIONE	ATTENUA	VALORI FINALI DI I & P
Mancato rispetto regole di minimizzazione, generalizzazione ed anonimizzazione	Formazione generale e specifica in tema protezione dati a tutto il personale	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti	P	I: Significativo P: Improbabile
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento	P	
	Attuazione delle procedure di Privacy by design	Rendere i dati pseudonimizzati e ove possibile anonimi.	P/I	
Violazione normativa	Formazione generale e specifica in tema	Tutto il personale ha ricevuto un doppio livello di formazione relativa alla protezione dei dati personali: il primo introduttivo ai principi e	P	I: Significativo

privacy, diritti e libertà degli interessati.	protezione dati a tutto il personale	all'organizzazione data protection della PLV, il secondo riguardante un approfondimento specifico per area tematica (in questo caso relativo all'attività di ricerca medica, biomedica ed epidemiologica) e la risoluzione di perplessità e dubbi concreti		P: Improbabile
	Autorizzazione al trattamento dei dati per tutto il personale	Tutto il personale è stato formalmente autorizzato al trattamento dei dati personali nel rispetto del modello organizzativo per la protezione dei dati personali della PLV	P/I	
	Supporto diretto dell'Ufficio Privacy con designati e autorizzati al trattamento	Il modello organizzativo per la protezione dei dati personali della PLV prevede la possibilità per i designati al trattamento di ricevere supporto diretto dell'Ufficio Privacy. L'Ufficio Privacy si è sempre reso disponibile a fornire supporto diretto anche ai soggetti autorizzati al trattamento	P	
	Attuazione procedure privacy by design	Rendere i dati pseudonimizzati e ove possibile anonimi	P/I	
Mancato controllo di qualità di informazioni generate	Formazione generale e specifica in utilizzo di IA	Tutto il personale ha ricevuto formazione relativa all'utilizzo di IA, nello specifico come effettuare controlli di qualità sulle informazioni generate.	I	I: Minimo P: Possibile

6. Eventuali osservazioni in merito alla necessità di adottare ulteriori misure di sicurezza

I livelli di RR rilevati nel presente documento consentono alla PLV di ritenere sicuri i trattamenti relativi alle attività di ricerca medica, biomedica ed epidemiologica svolte presso l'IRRCS.

Si segnalano, però, i seguenti elementi di criticità che, pur in un contesto di RR estremamente contenuto, vanno considerati:

1) Previsione di crittografia a riposo per tutti i dati contenuti sui database dell'area ricerca, il sistema di crittografia in uso è quello proposto dalla soluzione Sophos, attualmente utilizzato solo sulle postazioni laptop aziendali (windows); questo esclude la criptazione a livello di filesystem dalle restanti macchine (server, PC fissi, Workstation Linux,…);
2) Esecuzione di un vulnerability assessment per l'intera struttura dell'IRCCS,dopo aver messo in opera le azioni di rafforzamento della sicurezza informatica.

Infine, la PLV fa presente che sono in partenza due importanti progetti di compliance aziendale: adeguamento allo schema di certificazione UNI CEI EN ISO/IEC 27001:2022 inoltre siamo stati dichiarati "Soggetti Essenziali" relativamente alla Direttiva UE 2022/2555 (NIS2) e relativo D.Lgs 138/2024 di recepimento della stessa. La conclusione di questi processi di adeguamento andrà ulteriormente a rafforzare la sicurezza dei trattamenti esaminati nel presente documento.

7. Processo di approvazione e nuove versioni

La presente valutazione generale d'impatto è redatta dall'Ufficio Privacy della PLV, sentito il Referente Privacy locale e i designati al trattamento dei laboratori e delle unità di ricerca dell'IRCCS; la bozza definitiva è condivisa con il DPO, il quale ha la possibilità formulare un parere non vincolante (ma che necessita di apposito verbale di discostamento redatto dall'Ufficio Privacy nel caso in cui quest'ultimo decida di non seguire quanto indicato dal primo – vedi Procedura PR-PRY-005).

L'Ufficio Privacy si impegna a valutare il contenuto del presente documento al verificarsi delle seguenti condizioni (alternative tra loro):

- Allo scadere di un anno dall'approvazione dell'ultima versione del presente documento;
- Dopo l'aggiornamento del registro delle attività di trattamento del Titolare per la parte relativa ai laboratori, alle unità e ai servizi di ricerca dell'IRCCS;
- Al modificarsi delle attività e condizioni descritte ai punti 2 e 3 del presente documento;
- Al modificarsi dei valori riportati nelle analisi di cui ai punti 4 e 5 del presente documento.

Per la verifica, l'Ufficio Privacy valuta il coinvolgimento del Referente Privacy locale e/o dei designati al trattamento dei laboratori, delle unità e dei servizi di ricerca dell'IRCCS. L'Ufficio Privacy interpellerà nuovamente il DPO solo nel caso in cui, dopo la verifica, provveda a modificare la presente DPIA generale ai punti 3, 4 o 5 (tranne nelle ipotesi in cui la modifica sia meramente estetica o non alterante gli elementi indicati nel registro delle attività di trattamento del Titolare).

Il documento è approvato, in prima versione e per le modifiche dall'ufficio privacy.