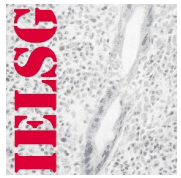
INTERNATIONAL EXTRANODAL LYMPHOMA STUDY GROUP

Valutazione di Impatto DPIA trattamento dati

Data: 22.07.2024



INTERNATIONAL EXTRANODAL LYMPHOMA STUDY GROUP

Indice

CONTESTO 4
PANORAMICA DEL TRATTAMENTO 4
DATI, PROCESSI E RISORSE DI SUPPORTO 5
PRINCIPI FONDAMENTALI 8
RISCHI 13
MISURE ESISTENTI O PIANIFICATE 13
ACCESSO ILLEGITTIMO AI DATI 21
MODIFICHE INDESIDERATE DEI DATI 22
PERDITA DI DATI 23
ANNEX A 25

Acronimi

DPO	Responsabile della Protezione dei Dati
EDPB	Comitato Europeo per la Protezione dei Dati
EOC	Ente Ospedaliero Cantonale
GDPR	Regolamento Generale sulla Protezione dei Dati
IELSG	International Extranodal Lymphoma Study Group
IOR	Istituto Oncologico di Ricerca
NMZL	Linfoma della Zona Marginale Nodale

CONTESTO

Questa sezione permette una visione complessiva del trattamento o dei trattamenti di dati personali in questione.

PANORAMICA DEL TRATTAMENTO

Questa sezione permette di individuare e presentare l'oggetto dell'analisi.

Domanda	Risposta	Stakeholder assegnatario	Scadenza	Note
Qual è il trattamento in considerazione? Presentare sinteticamente il trattamento: denominazione, finalità, risultati attesi, contesto di utilizzo, ed eventuali problematiche.	La presente analisi riguarda il trattamento dei dati personali dei pazienti all'interno dello studio clinico denominato IELSG52. Lo studio ha la finalità scientifica di identificare nuovi biomarcatori diagnostici e vulnerabilità terapeutiche del linfoma nodale della zona marginale al fine di consentire migliori opzioni di cura e trattamento. Per raggiungere tale scopo verranno analizzati, utilizzando i più moderni approcci di biologia molecolare, campioni biologici di un numero di pazienti pari ad almeno 500. I dati clinici dei pazienti verranno raccolti da centri localizzati in diversi paesi dell'Unione Europea, in India e negli Stati Uniti. Si precisa che lo studio si basa sull'analisi di campioni biologici raccolti per finalità di cura e poi riutilizzati previo consenso informato del paziente per le finalità di ricerca sopra indicate. Verranno altresì utilizzati campioni raccolti da pazienti deceduti. Come chiarito nel protocollo di studio l'utilizzo di tali campioni è necessario sia per una ragione quantitativa in quanto per raggiungere le finalità dello studio risulta necessario analizzare un numero di campioni maggiore rispetto a quello che si avrebbe a disposizione senza l'utilizzo dei campioni dei pazienti deceduti, sia perché quest'ultimi campioni forniscono delle informazioni proprio per il decesso dei pazienti utili e necessari allo studio pe raggiungere le sue finalità.			

Quali sono le responsabilità connesse al trattamento? Descrivere le responsabilità dei soggetti coinvolti: il titolare del trattamento, gli eventuali responsabili e contitolari.	Le attribuzioni di responsabilità nel trattamento dei dati sono connesse con il ruolo rivestito dai diversi soggetti all'interno della ricerca clinica. International Extranodal Lymphoma Study Group (IELSG) risulta essere il promotore dello studio e il Titolare del trattamento e si assume di conseguenza l'onere di verificare e controllare che i dati siano trattati nel rispetto della normativa. Anche i centri ove verrà svolta la ricerca saranno autonomi titolari del trattamento e verranno scelti dal promotore in base alla serietà e alle garanzie fornite anche in tema di trattamento dei dati. Le analisi dei campioni verranno svolte dall'Istituto Oncologico di Ricerca (IOR), nominato responsabile del trattamento dei dati ai sensi dell'art. 28 GDPR. I dati clinici verranno poi conservati sui server dell'Ente Ospedaliero Cantonale di Bellinzona (EOC) e i dati dei campioni biologi sui server dello IOR entrambi responsabili del trattamento dei dati. Allo stesso modo sono stati nominati soggetti autorizzati al trattamento ai sensi dell'art. 29 del GDPR il principale investigator i data manager e in generale chiunque agisca o tratti i dati sotto l'autorità del titolare.			
Ci sono standard applicabili al trattamento? Elencare gli standard rilevanti applicabili al trattamento, in quanto utili o obbligatori, specialmente i codici di condotta approvati e le certificazioni in materia di protezione dati.	Lo studio clinico nel trattamento dei dati dei pazienti si è uniformata alla normativa svizzera in materia di privacy, al GDPR e alle linee guida stabilite in materia dall'EDPB.			

DATI, PROCESSI E RISORSE DI SUPPORTO

Questa sezione permette di definire e descrivere nei dettagli il trattamento in oggetto.

Domanda	Risposta	Stakeholder assegnatario	Scadenza	Note

Quali sono i dati trattati? Elencare i dati raccolti e trattati indicando il periodo di conservazione, i destinatari e le persone che possono accedervi. Definire e descrivere l'ambito in dettaglio: - i dati personali in questione, i loro destinatari e i periodi di conservazione	Dati comuni: anno di nascita, genere Dati appartenenti a categorie particolari: dati clinici personali attinenti allo stato di salute fisica o mentale, dati genetici idonei a rivelare informazioni relative allo stato di salute o ad informazioni univoche sulla fisiologia dell'interessato, con specifico riferimento al materiale biologico del tumore del paziente e ai dati di salute relativi al linfoma. I dati clinici come anche i dati biologici saranno conservati per un periodo di tempo non superiore a quello necessario allo scopo per il quale sono stati raccolti nel rispetto della finalità di ricerca per cui vengono raccolti ed utilizzati, nel rispetto delle tempistiche normativamente previste per tale tipologia di trattamento e comunque per un periodo non superiore a un anno dalla fine dello studio. I dati saranno disponibili (nelle modalità e nei limiti che meglio si vedranno al punto che segue) unicamente ai medici che si occupano dello studio, ai ricercatori, al comitato etico di riferimento per lo studio, alle autorità regolatorie. L'eventuale diffusione dei dati della ricerca attraverso pubblicazioni scientifiche o in convegni scientifici avverrà in forma rigorosamente anonima.			
Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)? Descrivere il ciclo di vita dei dati (dalla raccolta alla distruzione, passando per la loro conservazione, i vari step del trattamento, l'archiviazione, ecc.), servendosi per esempio di un diagramma di flusso dei dati (che potete allegare) e fornendo una dettagliata descrizione di ciascun processo	Nell'ambito del trattamento medico di cura seguito dal paziente viene prelevato per scopi diagnostici o curativi del materiale tumorale dal linfonodo. Quando il materiale biologico prelavato non sarà più utile per le finalità diagnostiche e curative tale materiale potrebbe essere riutilizzo per gli scopi di cui alla presente ricerca. Questo avverrà qualora il paziente, se in vita, fornirà apposito consenso per il riutilizzo del suo materiale biologico e dei suoi dati sanitari relativi al linfonodo per le finalità di cui alla ricerca. Per i dati di pazienti deceduti, per cui non sia quindi possibile ottenere il consenso, l'utilizzo dei campioni verrà effettuato nel rispetto della normativa in vigore e quindi previa approvazione			

effettuato.	della ricerca da parte del comitato etico e previa dichiarazione e valutazione della necessità di utilizzare tali campioni e redazione di una dichiarazione di impatto. L'analisi e l'utilizzo dei campioni non avverrà in forma anonima in quanto risulta comunque sempre necessario mantenere aperta la possibilità di ricondurre i dati ottenuti ad un determinato paziente. I dati, tuttavia, verranno pseudo-anonimizzati in modo tale da rendere di fatto estremamente difficile, salvo necessità, risalire al nome del paziente che ha messo il campione a disposizione. I campioni riceveranno infatti un doppio livello di pseudo-anonimizzazione. Il medico attribuirà infatti sin da principio ai pazienti un codice alfanumerico, successivamente al momento del trasferimento dei campioni dal centro al promotore a quei campioni verrà attribuito altro codice alfanumerico collegato al primo codice attribuito dal centro. Dal momento dell'invio i dati del paziente saranno trasmessi registrati, elaborati e conservati unitamente a tale codice, alla sua data di nascita e al sesso. Soltanto il medico e i soggetti autorizzati potranno collegare questo codice al nominativo del paziente.			
Quali sono le risorse di supporto ai dati? Elencare le risorse che ospitano i dati oggetto del trattamento (sistemi operativi, server, software, reti, persone, supporti cartacei ecc.). Risorse dedicate al trattamento dei dati: le risorse su cui si basano i trattamenti dei dati personali. Nota: possono comprendere hardware, software, reti, persone, supporti cartacei o documentazione.	I dati clinici vengono inseriti in un software, Open Clinica, e memorizzati esclusivamente su un server centrale ospitato e gestito dall' EOC. I dati biologici verranno raccolti in softwares ospitati e gestiti dallo IOR. Tutti i servers si trovano in aree riservate ed il loro accesso è controllato attraverso un sistema dedicato e viene mantenuto un registro degli accessi. Né i programmi né le sezioni di programma sono memorizzati su computer locali dei siti partecipanti.			

PRINCIPI FONDAMENTALI

Questa sezione permette di generare lo schema di adeguamento secondo i principi di protezione dei dati personali.

Domanda	Risposta	Stakeholder assegnatario	Scadenza	Note
Gli scopi del trattamento sono specifici, espliciti e legittimi? Spiegare perché le finalità del trattamento sono specifiche, esplicite e legittime.	Le finalità di trattamento sono identificate nel fine di ricerca scientifica avente ad oggetto il miglioramento nella diagnosi e nella cura del linfoma nodale della zona marginale (NMZL). Più nello specifico la finalità scientifica dello studio è quella di identificare nuovi biomarcatori diagnostici e di migliore le cure del linfoma nodale della zona marginale. La valenza scientifica dello studio viene valutata dal comitato etico competente il cui assenso sarà condizione indispensabile per l'inizio dello studio.			
I dati personali devono essere raccolti per scopi specificati, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi. Vedi l'art. 5.1 b) del GDPR	I dati sono stati originariamente raccolti per finalità di cura del paziente; l'ulteriore utilizzo dei dati per finalità di ricerca è consentito ai sensi dell'art. 5.1 lett. b) ed ai pazienti in vita è chiesto preventivo consenso all'ulteriore trattamento dei propri dati per finalità di ricerca.			
Quali sono le basi legali che rendono lecito il trattamento? Presentare le basi legali del trattamento (ad esempio consenso, esecuzione di un contratto, obbligo legale, interessi vitali ecc.). Fondamenti di liceità - L'interessato ha acconsentito al trattamento dei propri dati personali per uno o più scopi specifici. - Il trattamento è necessario per l'esecuzione di un contratto di cui l'interessato è parte o per l'esecuzione di	La base legali del trattamento dei dati è ai sensi dell'articolo 6 lett. a) GDPR e art. 9 lett. a) GDPR il consenso esplicito espresso dall'interessato. Ove l'interessato non possa più essere contattato a seguito del suo decesso la base giuridica del trattamento viene ravvisato nel disposto dell'art. 9 lett. j) GDPR, nel rispetto di quanto indicato dall'articolo 110 del codice della privacy italiano così come modificato.			

misure adottate su richiesta dell'interessato prima di stipulare un contratto - Il trattamento è necessario per adempiere a un obbligo legale a cui è soggetto il titolare del trattamento - Il trattamento è necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica - Il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o connesso all'esercizio di pubblici poteri conferiti al titolare del trattamento - Il trattamento è necessario ai fini degli interessi legittimi perseguiti dal titolare del trattamento o da una terza parte, eccetto laddove prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore Vedi l'art. 6 del [GDPR]				
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? Spiegare perché ogni dato raccolto è necessario per le finalità del trattamento. Si tratta di ridurre la gravità dei rischi limitando la raccolta di dati personali al minimo necessario per la specifica finalità. Evitare di raccogliere dati non	I dati genetici raccolti dal materiale biologico del tumore sono essenziali per poter effettuare gli studi richiesti dalla ricerca in questione relativa all'identificazione di nuovi biomarcatori diagnostici. Sul punto è chiaro il protocollo dello studio che spiega anche le finalità e le ragioni per cui sia necessario analizzare anche i campioni di persone decedute. Nel trattamento dei dati sarà rispettato il principio di necessità per cui verranno trattati unicamente i dati essenziali per il raggiungimento delle finalità dello studio ossia nello specifico:			

necessari, di utilizzare dati che non abbiano alcun rapporto con la specifica finalità e di produrre impatti eccessivi sulle persone.	i dati di salute concernenti il linfoma ai fini di poter adeguatamente interpretare i dati provenienti dall'analisi del campione biologico, l'anno di nascita e il sesso del paziente. Gli ulteriori dati personali non sono essenziali al fine dello studio e pertanto non verranno utilizzati. Il paziente sarà quindi identificato, come si è già avuto modo di spiegare, da un doppio livello di pseudo-anonimizzazione che garantisce nel modo più profondo possibile i diritti di riservatezza del paziente.			
I dati sono esatti e aggiornati? Descrivere le misure previste per garantire la qualità dei dati.	I dati sono raccolti da medici esperti e competenti le cui capacità sono state valutate e ritenute idonee dal comito etico di riferimento. La professionalità attestata delle persone coinvolte costituisce garanzie della corretta modalità di ottenimento dei dati necessari per la ricerca.			
Qual è il periodo di conservazione dei dati? Spiegare perché il periodo di conservazione previsto per ogni dato sia necessario al raggiungimento delle finalità del trattamento, salva l'esistenza di un altro obbligo di legge che impone uno specifico termine di conservazione.	I dati saranno conservati per un periodo di tempo non superiore a quello necessario agli scopi di ricerca per i quali sono stati utilizzati nel rispetto delle norme di legge che regolano la materia in oggetto e comunque per un periodo non superiore ai 10 anni.			
Come sono informati del trattamento gli interessati? Descrivere le informazioni che si prevede di fornire agli interessati e gli strumenti utilizzati a tale scopo. Si tratta di garantire l'informazione delle persone e quindi di evitare la raccolta di dati a loro insaputa, verificando che il trattamento non sia soggetto a un'eccezione all'obbligo di informativa o a	Agli interessati viene fornita apposita informativa relativa al trattamento dei dati e connesso modulo di consenso informato dal medico prima che i dati siano trasferiti e utilizzati dal promotore per le citate finalità di ricerca. I dati dei pazienti deceduti per cui non sarà evidentemente possibile raccogliere il consenso verranno utilizzato nel rispetto della normativa già più volte citata.			

condizioni particolari.				
Ove applicabile: come si ottiene il consenso degli interessati? Descrivere le modalità previste per ottenere il consenso degli interessati. Si tratta di permettere ai soggetti interessati di dare un consenso libero, specifico e informato; verificare che una delle basi legali del trattamento sia il consenso, come previsto all'art. 6 del [GDPR]. Consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Vedi art. 4.10 del [GDPR]	Il consenso viene richiesto dal medico curante con apposito modulo e previa consegna della informativa. Il medico curante spiegherà al paziente le finalità della ricerca e il paziente deciderà se dare o non dare il consenso all'utilizzo dei suoi dati. Le modalità di ottenimento del consenso sono state valutate e approvate dai comitati etici a cui lo studio è stato sottoposto.			
Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati? Descrivere le modalità volte a consentire agli interessati di accedere ai propri dati e di riceverli o trasmetterli.	L'interessato può esercitare il suo diritto contattando il Titolare del trattamento il Centro di Sperimentazione nella persona del medico indicato nella informativa consegnata al paziente o comunque tramite il medico potrà rivolgersi direttamente a IELSG. I dati di contatto di Titolare e DPO sono indicati nell'informativa. L'informativa, quindi, contiene ogni specifica indicazione. Anche l'informativa è stata predisposta e sottoposta al comitato etico di riferimento per le dovute verifiche.			

Come fanno gli interessati a esercitare i loro diritti di rettifica, di cancellazione (diritto all'oblio), di limitazione e di opposizione? Descrivere le modalità volte a consentire agli interessati di rettificare e cancellare i loro dati.	L'interessato può esercitare il suo diritto contattando il Titolare del trattamento, il Centro di Sperimentazione nella persona del medico indicato nella informativa consegnata al paziente o comunque tramite il medico potrà rivolgersi direttamente al IELSG. I dati di contatto di Titolare e DPO sono indicati nella informativa. L'informativa, quindi, contiene ogni specifica indicazione. Anche l'informativa è stata predisposta e sottoposta al comitato etico di riferimento per le dovute verifiche.			
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto? Per ogni responsabile del trattamento, descrivere l'ambito delle rispettive responsabilità e specificare i riferimenti ai contratti, ai codici di condotta e alle certificazioni ove sono fissati gli obblighi loro incombenti.	Sì gli obblighi dei responsabili del trattamento sono disciplinati con chiarezza in un apposito accordo per il trattamento dei dati personali (cfr. art. 28 del GDPR).			
In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente? Per ogni Paese extra-UE dove i dati sono conservati o trattati, indicare e descrivere se si tratti di un Paese di cui è stata riconosciuta l'adeguatezza ovvero descrivere le condizioni che si applicano al trasferimento. A seconda del Paese in questione, si dovrà giustificare la scelta di conservare i dati al di fuori dell'UE e indicare le salvaguardie legali implementate al fine di	I dati sono trasferiti in Svizzera, paese terzo la cui normativa da poco rivista e che di fatto riprende interamente quelle del GDPR La Svizzera è considerato dalla Commissione Europea paese con un adeguato livello di sicurezza ed è stata pertanto parificata agli stati facenti parti della Comunità europea.			

garantire un'adeguata protezione dei dati oggetto di trasferimento oltre frontiera. Cioè: - Verso uno Stato membro dell'Unione Europea. - Verso un Paese con protezione adeguata riconosciuta dall'UE - Verso gli Stati Uniti a una società che ha aderito al Privacy Shield - Verso un altro Paese Vedi gli artt. 44-49 del [GDPR]				

RISCHI

Questa sezione permette di valutare i rischi per la riservatezza, alla luce delle misure esistenti o pianificate.

MISURE ESISTENTI O PIANIFICATE

Questa sezione permette di indicare le misure (esistenti o pianificate) che contribuiscono alla sicurezza dei dati

Domanda	Risposta	Stakeholder assegnatario	Scadenza	Note
Crittografia Descrivere gli strumenti crittografici implementati per assicurare la confidenzialità e l'integrità dei dati	I dati clinici sono trasmessi esclusivamente con crittografia SSL. Inoltre, vengono regolarmente specchiati e conservati in forma criptata tramite almeno due supporti dati esterni sicuri. I dati biologici grezzi del sequenziamento saranno archiviati in formato FASTQ. Verrà generato un file di metadati per collegare ogni file FASTQ al rispettivo paziente e time-point.			

Anonimizzazione e cancellazione del dato Indicare i meccanismi di anonimizzazione implementati	Durante il periodo di esecuzione dello studio i dati vengono utilizzati in forma pseudo-anonimizzati come descritto. Al termine del periodo di conservazione i dati verranno cancellati e distrutti. In ambito digitale i dati si dovranno cancellare impostando un blocco permanente che ne inibisca uso e lettura			
Partizionamento Indicare se sono pianificati partizionamenti del trattamento e come sono effettuati	Non sono previsti partizionamenti			
Controllo degli accessi logici Indicare come sono definiti e attribuiti i profili degli utenti	Dati clinici: i dati clinici verranno poi conservati sui server dell'EOC a cui è stata affidata la gestione informatica del dato nel rispetto della normativa e delle misure di sicurezza che l'Ospedale attua presso la sua struttura. L'accesso a tali dati da parte del promotore soggetto ad una modalità di autenticazione a due fattori. Dati biologici: i dati biologici dati dei campioni biologi sui server dello IOR a cui è stata delegata la gestione e la protezione dei dati.			
Tracciabilità Indicare se gli eventi sono registrati e il periodo di conservazione delle registrazioni	Dati clinici: un sistema di *audit trail* salva le procedure di accesso e documentazione nell'e-CRF. I dati vengono salvati ogni 24 ore. Dati biologici: per ogni campione, i dati grezzi del sequenziamento saranno archiviati in formato FASTQ. Verrà generato un file di metadati per collegare ogni file FASTQ al rispettivo paziente e punto di riferimento temporale. I dati dell'analisi delle immagini saranno archiviati come file originale #.tif e come file *.pdf.			

Archiviazione Indicare l'insieme dei meccanismi implementati per la conservazione e la gestione di archivi elettronici contenenti dati personali	n/a			
Sicurezza dei documenti cartacei Indicare le procedure relative al ciclo di vita dei documenti cartacei contenenti dati personali	n/a			
Minimizzazione dei dati Indicare i metodi implementati per ridurre il potenziale identificativo dei dati personali	Come si è già avuto modo di indicare viene attuata una doppia pseudo-anonimizzazione del dato. Presso il centro clinico ove il dato è raccolto, il paziente viene indicato con un codice alfanumerico. Il file che consente di associare il nome del paziente al codice alfanumerico che viene a lui assegnato viene conservato presso il centro in server separato rispetto a quello in cui sono conservati i dati del paziente in forma pseudo-anonimizzata. Al momento della comunicazione dei dati al promotore viene effettuata un'ulteriore pseudo-anonimizzazione per cui al paziente viene attribuito altro codice alfanumerico diverso dal primo. Il file che collega il secondo codice alfanumerico con il primo viene conservato dal promotore. Tale doppia pseudo-anonimizzazione rende di fatto quasi impossibile risalire se non per espressa volontà delle parti e quindi in caso di necessità ed unicamente da persone autorizzate. I dati personali e clinici trattati sono poi quelli necessari alla corretta esecuzione del protocollo clinico.			

Vulnerabilità Descrivere gli strumenti impiegati per garantire l'aggiornamento e il livello di sicurezza dei software utilizzati	Verranno utilizzati software di gestione delle patch, che consentono di identificare e applicare le patch di sicurezza rilasciate dai fornitori. Inoltre, i sistemi di gestione delle configurazioni controlleranno e monitoreranno le versioni del software installate, consentendo di identificare eventuali vulnerabilità o versioni obsolete. Verranno eseguite scansioni di sicurezza automatizzate per individuare potenziali vulnerabilità e falle di sicurezza. Infine, verranno eseguite attività di *penetration testing* per valutare la resistenza del software agli attacchi e identificare eventuali punti deboli.			
Lotta contro il malware Descrivere i controlli implementati contro il codice malevolo (malware) quando si accede a reti con un livello di sicurezza inferiore	Per evitare che i dispositivi vengano infettati da malware sono adottate le seguenti misure di sicurezza: - installazione di software antivirus - installazione di un firewall - aggiornamento regolare del software - regolare backup dei dati			
Gestione postazioni Descrivere le misure adottate al fine di ridurre i rischi di attacchi ai software utilizzati per il trattamento	Le misure di sicurezza adottate per proteggere il sistema riducendo i rischi di attacchi includono principalmente la crittografia, l'uso dell'autenticazione a due fattori, l'aggiornamento regolare del software, effettuare un backup regolare e l'utilizzo di password forti e complesse. Inoltre, deve presentare una infrastruttura adeguata che include firewall e software antivirus.			
Sicurezza dei siti web Descrivere metodi e strumenti implementati per proteggere i siti web	Non sono utilizzati siti web nel trattamento dei dati dello studio.			

Backup Indicare come sono gestiti e conservati i backup	Dati clinici: vengono utilizzati 2 sistemi di backup, uno settimanale ed uno giornaliero. Dati biologici: le procedure di backup sono conformi al livello RAID 5 oltre a una copia di backup archiviata nei server della rete IOR.			
Manutenzione Descrivere come è gestita la manutenzione fisica dei dispositivi	Tutti i dispositivi verranno aggiornati con le ultime patch di sicurezza e gli aggiornamenti del firmware. Piani di di manutenzione preventiva verranno eseguiti per compiere interventi regolari per la sostituzione delle parti usurabili (hard disk). Infine, un registro dettagliato delle attività svolte e delle eventuali riparazioni effettuate verrà creato.			
Contratto con il responsabile del trattamento Descrivere le garanzie contrattuali a tutela dei dati personali affidati a responsabili del trattamento	Le garanzie contrattuali a tutela dei dati personali affidate ai responsabili del trattamento sono descritte nei contratti di nomina a responsabile del trattamento all'EOC e allo IOR.			
Sicurezza dei canali informatici Indicare i controlli di sicurezza della rete sulla quale il trattamento è effettuato	I canali informatici di collegamento tra il Promotore e i soggetti incaricati per la conservazione e gestione dei dati clinici e genetici saranno protetti da Firewall e sistemi di rilevamento delle intrusioni che monitoreranno e filtreranno l'accesso ai dati, proteggendo la rete da attacchi esterni. Il promotore consentirà l'accesso ai dati unicamente a persone autorizzate e mediante un sistema di autenticazione con l'uso di password complesse e l'autenticazione a due fattori, in modo da ridurre sensibilmente il rischio di accessi non autorizzati.			
Controllo degli accessi fisici Indicare in che modo si realizza il controllo dell'accesso fisico ai locali che ospitano il trattamento	Tutti i servers si trovano in aree riservate ed il loro accesso è controllato attraverso un sistema dedicato e viene mantenuto un registro degli accessi			

Sicurezza dell'hardware Descrivere metodi e strumenti utilizzati per limitare i rischi posti alla sicurezza fisica di server e postazioni PC	Per limitare i rischi posti alla sicurezza fisica di server e postazioni PC l'accesso fisico é controllato con l'utilizzo di chiavi elettroniche o badge per l'ingresso in aree sensibili.			
Prevenzione delle fonti di rischio Descrivere metodi e strumenti utilizzati per evitare rischi di carattere generale	Gli ambienti dei server sono protetti da sistemi di videosorveglianza e allarmi antifurto.			
Protezione contro fonti di rischio non umane Descrivere le misure adottate per ridurre o prevenire i rischi connessi a fonti non umane	I server che conservano i dati sono alloggiati in stanze sicure, chiuse a chiave e dotate di controlli ambientali, come rilevatori di fumo e sistemi di condizionamento dell'aria per prevenire il surriscaldamento.			
Politica di tutela della privacy Descrivere come è strutturata l'organizzazione interna ai fini della tutela della vita privata	IELSG ha come missione il miglioramento della conoscenza e del trattamento dei linfomi attraverso la raccolta di dati, l'unione di scienziati provenienti da diverse parti del mondo e la ricerca clinica. La sua struttura è quindi organizzata al fine dell'esecuzione delle ricerche cliniche e del trattamento dei dati dei pazienti e si avvale per la conservazione del dato di soggetti competenti quale l'EOC e lo IOR alle quali ha delegato le attività gi gestione e conservazione del dato clinico e genetici nel rispetto delle rispettive competenze. IELSG non conserva quindi direttamente i dati, e i suoi collaboratori e dipendenti che vengono a contatto con i dati della ricerca clinica lo fanno collegandosi in modalità sicura al server dell'EOC a Bellinzona. IELSG quale titolare del trattamento e promotore dello studio clinico ha strutturato il trattamento in modo che il dato conservato non sia direttamente collegabile al paziente, ed anzi, ha predisposto un doppio sistema di			

	pseudo-anonimizzazione, già descritto, che rende di fatto tanto difficile il risalire ai dati identificativi del paziente dal rendere il trattamento assimilabile al trattamento di dati anonimi. IESLG ha implementato al suo interno una struttura privacy che rispetta i principi della privacy by design e della privacy by default previsti dal GDPR. Ha strutturato un organigramma privacy, attribuendo a ciascun soggetto una lettera di incarico rispettosa delle proprie mansioni e competenze, ha implementato le privacy policy necessarie ad una corretta gestione del data *breach* e al riscontro di richieste da parte degli interessati, ha nominato i soggetti a cui ha delegato attività responsabile del trattamento, ha predisposto il registro dei trattamenti, ha predisposto informative e, ove richiesto, consensi informati sottoposti per lo studio in oggetto al vaglio del comitato etico, ha applicato misure di sicurezza conformi e adeguate ai trattamenti effettuati.			
Gestione delle politiche di tutela della privacy Descrivere i metodi di gestione della base documentale per impostare gli obiettivi e le regole per la protezione dei dati	Nella gestione dei dati del presente studio IELSG utilizza i principi della data *protection* by design e by default. È stato predisposto un protocollo di studio, approvato dai relativi comitati etici, nei quali vengono indicate le finalità dello studio e i dati che devono essere trattati per il raggiungimento di tale finalità. Le informative e i consensi informati sono peraltro stati anch'essi analizzati e approvati dai comitati etici di riferimento. La gestione informatica del dato è stata delegata come più volte indicato. Il sistema di pseudo-anonimizzazione attuato rendere di fatto impossibile, se non per espressa volontà, risalire ai dati del paziente.			
Gestione dei rischi Descrivere i processi atti al controllo dei rischi che le operazioni di trattamento	Effettueremo una valutazione dei rischi, l'implementazione di misure di sicurezza adeguate e la supervisione continua. La valutazione dei rischi implica			

comportano per i diritti e le libertà degli interessati	l'identificazione delle potenziali minacce per i dati personali e l'analisi delle loro conseguenze. Le misure di sicurezza includono politiche e procedure di protezione dei dati, crittografia, controlli di accesso e formazione del personale. La supervisione continua assicura che le misure adottate siano efficaci nel prevenire violazioni dei dati e che vengano mantenute aggiornate in risposta a cambiamenti nel contesto operativo.			
Integrare la protezione della privacy nei progetti Descrivere in che modo si garantisce che la protezione dei dati personali sia tenuta in considerazione fin dalla fase iniziale di un nuovo progetto.	Il protocollo di studio, la gestione di informativa e consenso e la modalità di utilizzo dei dati è stata pensata sempre tenendo in considerazione la protezione dei dati dei pazienti.			
Gestire gli incidenti di sicurezza e le violazioni dei dati personali Descrivere i processi operativi volti a individuare e gestire gli eventi in grado di incidere sulle libertà e la privacy degli interessati.	Ogni segnalazione viene registrata in un apposito sistema di tracciamento e vengono informati i soggetti interessati. In caso di data *breach* IELSG ha implementato un processo di registrazione e analisi della problematica per assumere poi la decisione più appropriata nel rispetto della normativa e della tutela dei diritti dei pazienti.			
Gestione del personale Indicare le iniziative di sensibilizzazione del personale in materia di protezione dei dati attuate all'interno dell'azienda o dell'organismo	Si è provveduto alla formazione del personale in materia di protezione dei dati e sono state impartite istruzioni scritte al personale sulla tutela dei dati e sul corretto utilizzo degli strumenti aziendali.			
Gestione dei terzi che accedono ai dati Indicare, per i terzi autorizzati ad accedere ai dati, i controlli e le misure di sicurezza implementati su tali accessi	L'indicazione dei controlli e delle misure di sicurezza implementati per i terzi autorizzati includono l'autenticazione a più fattori, l'assegnazione di livelli di autorizzazione basati sui privilegi minimi necessari e l'uso di crittografia per la trasmissione e lo storage dei dati. Vi sarà una supervisione costante dell'accesso, registri di audit dettagliati e una rigorosa politica di			

	gestione delle password. La documentazione di tali controlli e misure fornisce trasparenza e favorisce la fiducia nell'affidabilità del sistema.			
Vigilanza sulla protezione dei dati Descrivere i processi finalizzati a svolgere verifiche periodiche sui trattamenti di dati	Verifiche periodiche verranno condotte e comprendono l'analisi dei registri di accesso, la revisione delle politiche e delle procedure, l'identificazione dei rischi di sicurezza e la valutazione dell'efficacia delle misure di sicurezza implementate. Inoltre, verranno condotti controlli sugli accessi autorizzati, la gestione dei dati sensibili e la corretta applicazione delle leggi sulla privacy. Le verifiche periodiche consentono di individuare eventuali vulnerabilità o violazioni e adottare le necessarie misure correttive per garantire la tutela dei dati personali.			
ACCESSO ILLEGITTIMO AI DATI Analizzare le cause e le conseguenze di accesso illegittimo ai dati, stimandone la gravità e la probabilità				
Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	La diffusione di dati particolari inerenti alla malattia del paziente e ai suoi dati sanitari.			
Quali sono le principali minacce che potrebbero concretizzare il rischio?	La principale minaccia riguarda l'accesso non autorizzato al dato tramite ingresso non autorizzato nel server presso cui i dati sono conservati, ovvero diffusione illegittima del dato a causa di errato trattamento dello stesso da parte di un soggetto incaricato al trattamento.			
Quali sono le fonti di rischio?	Le Fonti di rischio sono eventuali vulnerabilità del sistema informatico, errori da parte del personale che tratta i dati,			

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	Indicare: framework scelto, cifratura, standard di sicurezza sulle password, pseudo-anonimizzazione e procedure di manutenzione e aggiornamento software e hardware. In particolare, la doppia pseudo-anonimizzazione rende di fatto praticamente impossibile anche in caso di violazione dei sistemi informatici risalire al nome del paziente a cui i dati si riferiscono.			
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? Indefinito – Trascurabile – Limitato – Importante - Massimo	Il rischio vista la presenza della doppia pseudo-anonimizzazione dei dati, le misure di sicurezza assunte per la conservazione del dato, è ritenuto limitato.			
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Indefinito – Trascurabile – Limitato – Importante - Massimo	Limitato.			
MODIFICHE INDESIDERATE DEI DATI Analizzare le cause e le conseguenze di modifiche indesiderate dei dati, e stimare la gravità e la probabilità dell'evento.				
Domanda	**Risposta**	**Stakeholder assegnatario**	**Scadenza**	**Note**
Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?	La conseguente mancata attendibilità dei rilievi effettuati. Trattandosi tuttavia di rilievi relativi alle finalità di ricerca l'impatto di modifiche dei dati sull'interessato al trattamento sarebbe marginale.			

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?	L'accesso non autorizzato presso il server che contiene i dati con conseguente modifica degli stessi, l'errore umano di chi esegue e riporta i risultati delle analisi.			
Quali sono le fonti di rischio?	Eventuali vulnerabilità del sistema di protezione informatico e la figura dei soggetti che svolgono le analisi e che riportano i risultati delle stesse.			
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	Le misure di sicurezza assunte a protezione del sistema informatico, l'alta professionalità dei laboratori e dei soggetti coinvolti nello studio.			
Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate? Indefinito – Trascurabile – Limitato – Importante - Massimo	Il rischio è trascurabile.			
Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate? Indefinito – Trascurabile – Limitato – Importante - Massimo	Trascurabile			

PERDITA DI DATI

Analizzare le cause e le conseguenze di una perdita di dati stimandone la gravità e la probabilità

Domanda	**Risposta**	**Stakeholder assegnatario**	**Scadenza**	**Note**
Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?	La perdita dei dati potrebbe avere un impatto sull'interessato che non avrebbe più a disposizione dati sanitari relativi al suo stato di salute.			

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?	La principale minaccia riguarda l'accesso non autorizzato al dato tramite l'applicazione web o la distruzione del server.			
Quali sono le fonti di rischio?	Le fonti di rischio sono gli utenti di tipo "medico" e "referente del centro" ed eventuali vulnerabilità dell'applicazione web			
Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?	La cifratura dei dati, gli standard di sicurezza sulle password, la pseudo-anonimizzazione, le procedure di manutenzione e l'aggiornamento e il back up dei dati.			
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate? Indefinito – Trascurabile – Limitato – Importante - Massimo	Trascurabile			
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate? Indefinito – Trascurabile – Limitato – Importante - Massimo	Trascurabile			

ANNEX A – *Specifiche misure di sicurezza imposte all'interno delle prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016 dell'Autorità Garante per la protezione dei dati personali).*

Domanda	Risposta	Stakeholder assegnatario	Scadenza	Note
L'accesso ai locali ove vengono custoditi i campioni biologici è controllato anche mediante strumenti elettronici che prevedano specifiche procedure di identificazione che includono dispositivi biometrici?	L'accesso ai locali dove verranno custoditi i campioni biologici è controllato mediante impianto di video-sorveglianza ed è consentito solo mediante "badge" personale. Tutti gli accessi verranno registrati e salvati su appositi dispositivi elettronici.			
Le persone ammesse all'accesso a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate?	Qualsiasi accesso ai dati verrà tracciato in apposito log file.			
La conservazione, l'utilizzo e il trasporto dei campioni biologici sono posti in essere con modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità?	Il trasporto dei campioni avviene seguendo protocolli di sicurezza e utilizzando apposite soluzioni di conservazione. Inoltre, la tracciabilità è garantita attraverso l'etichettatura accurata e la documentazione dettagliata dei campioni, garantendo la rintracciabilità delle informazioni pertinenti a ogni fase del processo. Queste pratiche assicurano che i campioni biologici rimangano affidabili e utilizzabili per scopi futuri.			
Il trasferimento dei dati genetici, con sistemi di messaggistica elettronica ivi compresa la posta, è effettuato con le seguenti cautele	✓ trasmissione dei dati in forma di allegato e non come testo compreso nel corpo del messaggio; ✓ cifratura dei dati avendo cura di rendere nota al destinatario la chiave crittografica tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati; ✓ ricorso a canali di comunicazione protetti, tenendo conto dello stato dell'arte della tecnologia utilizzata; ✓ protezione dell'allegato con modalità idonee a impedire l'illecita o fortuita acquisizione dei dati trasmessi, come una password per l'apertura del file			

	resa nota al destinatario tramite canali di comunicazione differenti da quelli utilizzati per la trasmissione dei dati ✓ è ammesso il ricorso a canali di comunicazione di tipo "*web application*" che prevedano l'utilizzo di canali di trasmissione protetti, tenendo conto dello stato dell'arte della tecnologia, e garantiscano, previa verifica, l'identità digitale del server che eroga il servizio e della postazione client da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione			
In relazione alla consultazione dei dati genetici trattati con strumenti elettronici, la stessa è consentita previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note ai soggetti all'uopo designati e di dispositivi, anche biometrici, in loro possesso?	I dati genetici ed i campioni biologici contenuti in elenchi, registri o banche di dati, sono trattati con tecniche di cifratura o di pseudo-anonimizzazione o di altre soluzioni che, considerato il volume dei dati e dei campioni trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati siano tenuti con strumenti elettronici e contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate			
L'informativa da sottoporre ai soggetti interessati prima della raccolta dei campioni biologici evidenzia i requisiti di cui agli artt. 13 e 14 del GDPR e:	L'informativa da sottoporre è stata predisposta tenendo conto dei requisiti previsti nell'articolo 13 e 14 del GDPR. a) nell'informativa viene contemplata la possibilità di essere informati nel caso di risultati inattesi derivanti dalle analisi condotte sui campioni, se tali risultati			

a) i risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici? b) la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di questi dati per ulteriori scopi?	dovessero essere rilevanti per la salute del paziente. b) Non è previsto né il trasferimento dei campioni biologici raccolti per lo studio né il loro riutilizzo per ulteriori scopi.			