Valutazione di Impatto sulla protezione dei dati personali
Studio clinico su campione biologico TLS_LLC_Modena

Codice Documento: GDPR-PR15-20

Titolo Studio Clinico: Meccanismi molecolari della patogenesi della leucemia linfatica cronica(LLC).

Titolari autonomi coinvolti nello studio

- Centro: Azienda Ospedaliero-Universitaria di Modena
- Promotore: Fondazione Toscana Life Sciences

Autorizzazione Comitato Etico Azienda Ospedaliero-Universitaria di Modena: Prot. Nr. 1175/2026

Sommario

1 Introduzione

La DPIA, acronimo di *Data Protection Impact Assessment*, è una valutazione preliminare, eseguita dal Titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati. In linea con l'approccio basato sul rischio, adottato dal Regolamento generale sulla protezione dei dati Reg UE 2016/679 (di seguito anche "GDPR"), è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del GDPR).
Preso atto della tipologia di Studio su campione biologico (retrospettivo e prospettico), è condotta e resa pubblica una valutazione d'impatto sulla protezione dei dati, in forza dell'art. 35 del GDPR riguardo al trattamento dei dati ai sensi e per gli effetti del combinato disposto degli artt. 9, par. 2, lett. j) del GDPR, 110 e 110 bis, comma 4 del Codice Privacy.
La presente valutazione riporta:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Tenuto conto della natura, del contesto, delle finalità e dell'ambito di applicazione del trattamento in esame, il livello di rischio residuo, considerato accettabile indicato dal Titolare, sentito anche il parere del DPO, è risultato BASSO.

1.1 Recapiti del Promotore

Fondazione Toscana Life Sciences, Via Fiorentina, 1 53100 Siena; e-mail: privacy@toscanalifesciences.org; dpo@toscanalifesciences.org.

1.2 Definizioni e acronimi

ACRONIMO	DEFINIZIONE
FTLS	Fondazione Toscana Life Sciences
GDPR	Regolamento UE n. 2016/679
PI	Principal Investigator (Sperimentatore Principale)
CRF	Case Report Form
TMF	Trail Master File
ICF	Informed Consent Form
DPO	Data Protection Officer

TERMINE	DEFINIZIONE
Sponsor/Promotore	individuo, società, istituzione o organizzazione che si assume la responsabilità dell'avvio, della gestione e/o del finanziamento di una sperimentazione clinica.
Contract Research Organization/Organizzazione di Ricerca a Contratto	un'organizzazione con cui il promotore della sperimentazione ha stipulato un contratto o ha stipulato altra forma di accordo, per affidare alla stessa una parte o tutte le proprie competenze in

	tema di sperimentazione clinica, pur rimanendosi responsabile della stessa
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (art. 4, n. 13, GDPR).

2 Contesto e standard applicabili al trattamento

La presente Valutazione d'impatto della protezione dei dati (o DPIA) ha lo scopo di valutare i rischi per i soggetti inclusi nello studio clinico su campione biologico (di seguito anche lo "Studio"), promosso dalla Fondazione Toscana Life Sciences (di seguito anche lo "Sponsor" o il “Promotore”).

Questo Studio, classificato come monocentrico, no-profit, interventistico su campione biologico, senza farmaco né dispositivo medico, retrospettivo e prospettico, ha come obiettivo quello di valutare il ruolo del glucosio e del rame nello sviluppo della Leucemia Linfatica Cronica (LLC) e come questo può aiutare ad individuare nuovi trattamenti per la malattia.

Lo studio include componenti sia retrospettive che prospettiche.

- **Coorte retrospettiva:** per i campioni conservati presso i laboratori dell’Azienda Ospedaliero-Universitaria di Modena, raccolti nel periodo 2020-2024 e che presentano determinate caratteristiche biologico-molecolari, lo Sperimentatore Principale, o suo delegato, provvederà a ricontattare i pazienti donatori per illustrare il protocollo, sottomettere loro il consenso specifico per la partecipazione allo studio e al trattamento dati personali.

- **Coorte prospettiva:** Ai pazienti adulti affetti da LLC che eseguono presso la Struttura Complessa di Ematologia, A.O.U di Modena, le prime visite o quelle di follow-up programmate, verrà illustrato dallo Sperimentatore Principale o suo delegato, durante tali visite, il protocollo clinico e le attività di analisi dei campioni. Ai soggetti interessati verrà sottoposto alla firma il consenso alla partecipazione allo studio e al trattamento dei dati personali.

Lo studio sarà condotto secondo quanto indicato nel protocollo di studio (il "Protocollo") e riportato nell’ Informativa per il partecipante, nel Modulo di consenso informato ("ICF") alla partecipazione allo studio e al trattamento dei dati personali, che fanno parte della documentazione trasmessa e approvata dal Comitato Etico competente. Lo studio sarà condotto in accordo con i principi etici sanciti dalla Dichiarazione di Helsinki nella sua ultima revisione, dalla Convenzione sui Diritti dell'Uomo e la Biomedicina, nelle vigenti regole della Buona Pratica Clinica, e in conformità delle leggi applicabili in tema di trasparenza e prevenzione della corruzione, nonché di protezione dei dati personali secondo la normativa vigente, salvaguardando quindi i diritti sanciti dalla legge in materia di protezione dei dati personali (Decreto Legislativo 30/6/2003 n. 196 e successive modificazioni; Regolamento UE generale sulla protezione dei dati personali 679/2016).

Si ritiene necessaria una DPIA per valutare, lato Promotore, i rischi associati: a) al trattamento dei dati personali, anche particolari, dei pazienti pseudonimizzati nel contesto di progetti di ricerca o di sperimentazioni cliniche; b) al trattamento di dati personali riferiti alla coorte retrospettiva.

3 Panoramica del trattamento

Lo studio non prevede alcuna modifica dell’iter diagnostico e terapeutico del paziente. Lo studio prevede l’arruolamento di pazienti durante visite pianificate secondo pratica clinica. Al fine del protocollo, non viene richiesta nessuna procedura aggiuntiva rispetto alla pratica clinica, né ulteriori

valutazioni diagnostiche. I pazienti verranno arruolati nello studio in relazione alle caratteristiche di inclusione definite nel Protocollo.
Per ciascun paziente saranno collezionati dati clinici come da Case Report Form (CRF), autorizzata dal Comitato Etico competente.

Lo Sperimentatore Principale, o suo delegato, è responsabile dell'ottenimento e della conservazione del consenso informato scritto di ciascun partecipante allo Studio, dopo un'adeguata spiegazione degli obiettivi e dei metodi dello Studio stesso e prima di intraprendere qualsiasi procedura correlata al Protocollo. Infatti, l Sperimentatore principale, prima di iniziare la Sperimentazione, deve acquisire il consenso informato del paziente, o del suo rappresentante legale, secondo quanto previsto dalla vigente normativa in materia di sperimentazioni cliniche e il consenso al trattamento dei dati personali ai sensi e per gli effetti della vigente normativa nazionale e comunitaria in materia di protezione dei dati personali. Lo Sperimentatore principale deve informare in modo chiaro e completo, prima che abbia inizio la Sperimentazione (incluse le eventuali relative fasi prodromiche e di screening) ogni paziente circa natura, finalità, risultati, conseguenze, rischi e modalità del trattamento dei dati personali.

Il Promotore per mantenere la documentazione necessaria alla gestione in qualità dello studio archivia nel proprio TMF, previo consenso scritto al trattamento, anche i dati dello sperimentatore e del suo staff contenuti nei CVc condivisi, correlati con i dati di contatto.

4 Procedure di inclusione nello studio presso il Centro

Ai pazienti adulti affetti da LLC che eseguono, presso la Struttura Complessa di Ematologia, A.O.U di Modena, le prime visite o quelle di follow-up programmate, verrà illustrato dallo Sperimentatore Principale, o suo delegato, durante tali visite, il protocollo clinico e le attività di analisi dei campioni. Ai soggetti interessati verrà sottoposto alla firma il consenso alla partecipazione allo studio e al trattamento dei dati personali.

Per i campioni conservati presso i laboratori dell'Azienda Ospedaliero-Universitaria di Modena, raccolti nel periodo 2020-2024 e che presentano determinate caratteristiche biologico-molecolari, lo Sperimentatore Principale, o suo delegato, provvederà a ricontattare i pazienti donatori per illustrare il Protocollo di studio e sottomettere loro il consenso specifico alla partecipazione e al trattamento dati personali.

Il consenso informato scritto del paziente sarà raccolto dal PI o suo delegato in conformità al Provvedimento del Garante per la Protezione dei Dati Personali n. 146/2019, al Provvedimento 101 del 10/08/2018, al GDPR -Regolamento (UE) 679/2019-, e del Provvedimento del Garante per la protezione dei dati personali n. 298 del 09/05/2024 all'Autorizzazione Generale del Garante per la Protezione dei Dati Personali n. 9/2016 e al D.lgs 196/2003, articoli 110 e 110/bis inclusi. Per la sola coorte retrospettiva, questi ultimi in particolare sono applicabili nel caso in cui non risulti possibile l'acquisizione di uno specifico consenso da parte degli interessati inclusi nello studio a causa di motivi di impossibilità organizzativa riconducibili alla circostanza che, la mancata raccolta dei dati riferiti al numero di interessati che non è possibile contattare rispetto al numero complessivo dei soggetti che si intende arruolare nella ricerca, produrrebbe conseguenze significative per lo studio in termini di qualità dei risultati della ricerca stessa; ciò avuto riguardo, in particolare, ai criteri di inclusione previsti dallo studio, alle modalità di arruolamento, alla numerosità statistica del campione prescelto, nonché al periodo di tempo trascorso dal momento in cui i dati riferiti agli interessati sono stati originariamente raccolti. I motivi di impossibilità organizzativa concernono sia quelli derivanti dalla circostanza, da considerarsi del tutto residuale, che contattare gli interessati implicherebbe uno sforzo sproporzionato, sia quelli derivanti dalla circostanza, alternativa alla precedente, che all'esito di ogni

ragionevole sforzo compiuto per contattarli (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto pubblicamente accessibili) essi risultino al momento dell'arruolamento nello studio, deceduti o non contattabili. Resta fermo l'obbligo per il Centro di raccogliere il consenso al trattamento dei dati personali degli interessati inclusi nello studio in tutti i casi in cui, nel corso dello studio stesso, sia possibile rendere loro un'adeguata informativa e, in particolare, quando gli interessati si rivolgano al Centro di cura anche per prestazioni sanitarie, visite di controllo, ecc.

A dimostrazione dello sforzo profuso dal Centro, la lista dettagliata delle attività intraprese per la presentazione dello studio e la raccolta del consenso informato ai soggetti appartenenti alla Coorte retrospettiva verrà archiviata a cura del PI o suo Delegato.

Criteri di inclusione nello Studio (valutazione a cura del PI del Centro)

- Pazienti adulti con CLL alla diagnosi o in follow-up;
- Pazienti che abbiano firmato il consenso informato per la partecipazione allo studio e al trattamento dei dati personali (se appicabile)

Criteri di esclusione dell'arruolamento (valutazione a cura del PI del Centro)

- Qualunque condizione clinica che nella valutazione dello sperimentatore possa determinare un rischio al soggetto in conseguenza della partecipazione allo studio.
- Soggetti non disponibili a firmare il consenso informato;
- Già nota infezione da HIV, HCV e HBV.

Si prevede d'includere massimo 100 (cento) pazienti affetti da LLC, tra pazienti reclutati prospetticamente e retrospettivi.

5 Tipologia di dati personali trattati

I dati personali acquisiti e trattati sono limitati a quanto strettamente necessario per adempiere allo scopo scientifico dello studio o agli obblighi normativi.
L'identità dei pazienti è nota al PI e al suo Staff nell'ambito dello studio, ma non sarà condivisa con lo Sponsor. Tutti i dati dei pazienti sono collegati agli stessi tramite un codice alfanumerico identificativo e solo il Centro e/o lo Sperimentatore dispongono della chiave di decodifica che collega tale codice al singolo paziente. Né lo Sponsor né alcun fornitore riceverà una copia di tale chiave di decodifica.
L'eventuale Monitor dello Sponsor visiterà il Centro per esaminare che la conduzione dello Studio avvenga in conformità con il Protocollo e per condurre la verifica dei dati/documenti sorgente, avendo quindi accesso ai dati dei pazienti. I dati dei pazienti non verranno condivisi esternamente né con lo Sponsor nè con altri rappresentanti dello Sponsor e non verranno copiati né conservati su alcun supporto elettronico o cartaceo dal Monitor dello Studio.

5.1 Categoria di dati trattati presso il Centro (Titolare autonomo)

Presso il centro verranno acquisite dai pazienti inclusi nello studio le seguenti categorie di dati personali:

- nome, cognome, codice fiscale e dati di recapito;
- sesso e anno di nascita;
- dati relativi alla salute, ossia cartella clinica del paziente;
- codice pseudonimizzazione.

5.2 Categoria di dati trattati presso il Promotore (Titolare autonomo)

Presso lo Sponsor, da comunicazione sicura degli stessi da parte del Centro:

- Codice di pseudonimizzazione attributo al paziente;
- Dati sanitari presenti in CRF, età, sesso e informazioni genetiche;
- Dati identificativi, di contatto e informazioni contenute nei CVs del PI e dello Staff coinvolto nella sperimentazione

6 Basi giuridiche

Gli studi su campione biologico vengono sottoposti a parere del Comitato Etico territoriale, che valuta la documentazione presentata. Lo stesso fornisce la documentazione necessaria alla sottomissione, compresi i consensi e le informative al trattamento. Lo Sponsor e il Centro predispongono una convenzione per la conduzione dello studio che disciplina i ruoli e le responsabilità privacy.
L'autorizzazione al trattamento di dati personali, anche particolari, di soggetti inclusi nello studio avviene tramite espressione di consenso alla partecipazione allo studio e al trattamento dati personali, sia per la coorte prospettiva che per la coorte retrospettiva per i soggetti contattabili. Per i soggetti non contattabili o deceduti della coorte retrospettiva, il Centro effettuerà, come indicato nella sezione "Procedure di inclusione" del Protocollo di studio, ogni ragionevole e documentato sforzo (anche attraverso la verifica dello stato in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente forniti, nonché l'acquisizione dei dati di contatto pubblicamente accessibili) per presentare il Protocollo e raccogliere la firma al consenso al trattamento. Registro di tali attività verrà mantenuto presso il Centro.
Quindi

- *Paziente in prima visita o follow-up, paziente in vita e rintracciabile*

Art. 6 par. 1, lett. A) e Art. 9 par. 2 lett. a) del GDPR (acquisizione del consenso). Il consenso è raccolto dal paziente in fase di arruolamento, tramite l'acquisizione di firma autografa su ICF e Consenso al trattamento dati personali;

- *Pazienti deceduti o non rintracciabili*

Art. 9 par. 2 lett. j) del GDPR e artt. 110-110 bis c. 4 del d.lgs. 196/03 e Aut. Gen. 9/2016 e ss aggiornamenti: il trattamento è necessario a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea, ed è condotta e resa pubblica una valutazione d'impatto sulla protezione dei dati. L'interessato è qualificato come non rintracciabile dopo almeno 3 tentativi (tracciati) di contatto non riusciti. L'interessato deceduto viene rilevato dalla Cartella Clinica (in caso di decesso durante un periodo di degenza presso Azienda Ospedaliero-Universitaria di Modena) o dal sistema TS (tessera sanitaria). A dimostrazione dello sforzo profuso dal Centro, la lista dettagliata delle attività intraprese per la presentazione dello studio e la raccolta del consenso informato ai soggetti deceduti o non rintracciabili verrà archiviata a cura del PI o suo Delegato.

Il consenso al trattamento dei dati relativi al PI e ai membri del suo staff avviene tramite rilascio di consenso scritto.

7 Periodo di Conservazione dei dati

I dati personali trattati nell'ambito di studi interventistici (quelli cioè che prevedono la somministrazione di un farmaco in sperimentazione o l'utilizzo di dispositivo non ancora omologato) devono essere conservati per un periodo di 25 anni. Negli altri casi, i dati personali verranno conservati per almeno 7 anni, ovvero per un periodo di tempo considerevolmente più lungo in conformità alla disciplina applicabile o agli accordi intervenuti il promotore medesimo e centri partecipanti (art. 18 d.lg.

n. 200/2007;d.lg. n. 219/2006, all. 1, punto 5.2, lett. c); d.m. 15 luglio 1997, all. 1/4B, punti 4.9.4 e 4.9.5 e all. 1/5A, punti 5.5.11 e 5.5.12). Al termine dei periodi di conservazione, i dati personali saranno integralmente cancellati in modo irreversibile o resi anonimi.
La presente DPIA si riferisce a studi su campione biologico; quindi, la conservazione dei dati personali è di almeno 7(sette) anni successivi la chiusura dello studio, come anche da Protocollo e Convenzione con il Centro.

I dati personali, anche particolari, di origine e la tabella di decodifica (dati personali identificativi - codice univoco di pesudonimizzazione) vengono conservati nei locali e/o infrastruttura del Centro, sotto la responsabilità del PI di Studio.

Presso lo Sponsor, vengono conservati i dati pseudonimizzati e le informazioni presenti nella CRF approvata dal Comitato Etico competente, oltre ai Cvs e ai dati di contatto del PI e dei membri del suo Staff.

8 Condivisione dei dati

Lo Sperimentatore dello studio, o suo delegato, acquisce i dati dei soggetti coinvolti, conserva i documenti di origine e la chiave di decodifica, che collega il codice identificativo univoco del soggetto alla sua identità. La CRF riportante il codice di pseudonimizzazione verrà condivisa dal PI con lo Sponsor tramite posta elettronica aziendale, condividendo solo documenti crittografati con password, chiave di decifrazione condivisa con altro mezzo.
I dati personali dei soggetti inclusi pseudonimizzati che sono stati acquisiti durante lo studio possono essere condivisi solo con lo Sponsor, da questi, se previsto, con i propri fornitori (nominati dallo Sponsor responsabili esterni del trattamento, a seconda dei casi) e altri soggetti terzi, secondo quanto consentito dall'ICF e dal Protocollo, a meno che non sia consentito o previsto dalla legge, tra cui:

- autorità regolatorie;
- affiliati e fornitori dello Sponsor, compresi i laboratori e altri fornitori che partecipano alla conduzione e monitoraggio dello Studio.

Secondo la legge, alcuni soggetti potranno essere autorizzati ad accedere, presso il Centro, ai dati personali non codificati dei pazienti per verificare l'accuratezza e la validità dello studio o per ottemperare ad altri obblighi normativi. Tali soggetti sono vincolati contrattualmente alla riservatezza, e sono:

- autorità regolatorie;
- Monitor nominati dallo Sponsor.

9 Soggetti che accedono ai dati

Presso il Promotore:

- Responsabile della Sperimentazione e collaboratori
- Membri del Team Studi Clinici

Per l'archiviazione digitale, l'accesso alle cartelle di rete interna aziendale può avvenire, per fini di manutenzione e sicurezza dell'infrastruttura, anche da parte degli Amministratori di Sistema incaricati. Tutti i soggetti, tenuti alla riservatezza e confidenzialità per contratto, hanno ricevuto autorizzazione al trattamento con istruzioni alla gestione e sicurezza dei dati, oltre a formazione privacy almeno annuale e formazione GCP.

Eventuali fornitori di servizi di monitoraggio o laboratori terzi di analisi verranno nominati Responsabili Esterni al trattamento dati personali.

10 Trasferimento dei dati a soggetti terzi in paesi ExtraUE

Nessun dato verrà trasferito extra EU.

11 Minimizzazione dei dati

I dati personali raccolti sono solo quelli espressamente necessari all'esecuzione del protocollo di studio sottomesso e autorizzato. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).

12 Esercizio dei diritti

I soggetti partecipanti allo studio hanno il diritto di accedere ai loro dati personali trattati per lo studio e richiederne la rettifica, limitazione, eliminazione o esportazione. Inoltre, possono revocare il loro consenso alla partecipazione allo studio e alla raccolta di ulteriori dati in qualsiasi momento.

Per queste richieste, i soggetti dovranno contattare esclusivamente il medico responsabile dello studio o per iscritto l'Azienda Ospedaliero - Universitaria di Modena - Prof. Roberto Marasca, email: roberto.marasca@unimore.it. Senza il supporto del medico dello studio, infatti, lo Sponsor non è in grado di soddisfare alcuna richiesta dei soggetti partecipanti per la mancanza di informazioni (per es., quale serie di dati pseudonimizzati è correlata a ciascun partecipante). I soggetti partecipanti hanno il diritto di ritirarsi dallo studio in qualsiasi momento informando il medico responsabile dello studio. Lo Sponsor sarà informato dal medico dello studio della revoca del consenso alla partecipazione allo studio da parte di un soggetto e non saranno raccolte altre informazioni su di lui. Il soggetto partecipante allo studio può inoltre esercitare il diritto all'oblio (art. 17 del GDPR) e dunque richiedere la cancellazione di tutti i suoi dati personali raccolti trattati dallo Sponsor: tale diritto tuttavia potrebbe non essergli riconosciuto in tutto o in parte dallo Sponsor se la conservazione dei dati correlati risultasse necessaria per l'adempimento di un obbligo legale che richieda il trattamento di tali dati e/o nella misura in cui la loro cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi scientifici dello studio connessi al trattamento. Il soggetto partecipante ha comunque il diritto di presentare reclamo all'Autorità Garante per la protezione dei dati personali.

13 Misure a tutela dei diritti degli interessati

Il trattamento dei dati nell'ambito degli Studi potrebbe comportare conseguenze negative in caso di accessi non autorizzati ovvero qualora i dati venissero cancellati o alterati. Per ridurre la possibilità che tali eventi si verifichino, e la gravità delle conseguenze negative che ne potrebbero derivare, FTLS ha implementato idonee misure di sicurezza.

Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa, comprensiva dell'esercizio dei diritti, viene resa disponibile secondo le seguenti modalità:

• Consegna a cura del PI o suoi delegati, come da Convenzione con il Centro.

13.1 MISURE ORGANIZZATIVE

- Definizione di un gruppo dedicato alla gestione interna degli studi clinici e ai rapporti con Centri e Comitati Etici: personale formato in materia privacy almeno annualmente e certificato GCP, oltre che su proprietà intellettuale e sicurezza informativa.
- Personale del Team Privacy e DPO coinvolti nelle attività di trattamento per valutazioni e redazioni documentazioni e DPIA

- Formazione di tutto il personale interno coinvolto negli studi in materia privacy e GCP
- Definizione della gestione dell'archiviazione della documentazione
- Definizione della gestione della conservazione dei dati degli studi clinici
- Definizione delle attività di monitoraggio degli studi clinici
- Procedura per la gestione degli incidenti che possono comportare una violazione di dati ("Policy data breach").
- Definizione procedura per Deviazioni al Protocollo
- Redazione Regolamento Informatico e di accesso ai dati
- Nomina autorizzati al trattamento per personale coinvolto
- Formazione Studio specifica per tutto il personale del Centro coinvolto e per il personale dello Sponsor coinvolto su Protocollo e attività correlate.

13.2 MISURE DI SICUREZZA FISICA

La sicurezza fisica dei locali della FTLS è garantita da sistemi di videosorveglianza, controllo degli accessi da parte del personale della sicurezza (presente 24 ore su 24, 7 giorni su 7). Inoltre, i locali dove vengono effettuati i trattamenti più sensibili sono accessibil dal solo personale autorizzato mediante badge identificativo. I documenti sono inoltre conservati in armadi chiusi a chiave in locali con accesso controllato. Al TMF hanno accesso esclusivamente i membri del Team Studi Clinici.

13.3 MISURE TECNICHE

Ai sensi dell'art 32 GDPR, lo Sponsor dichiara le seguenti

MISURE DI SICUREZZA APPLICATE AL TRATTAMENTO		
MISURA	Esistenti	Note
Organigramma privacy	X	
Nomine responsabili esterni	Al momento della stesura della presente non necessari	
Nomina DPO	X	
Informativa	X	Consenso e informative, come da protocollo di Studio.
Istruzioni persone autorizzate trattamento	X	Le persone autorizzate al trattamento hanno ricevuto idonea nomina. Training di inizio studio sia per il personale del Promotore che per il personale del Centro per la corretta conduzione dello Studio. Certifica GCP.
Formazione	X	Training di inizio studio sia per il personale del Promotore che per il personale del Centro per la corretta conduzione dello Studio. Certifica GCP. Corso almeno annuale in ambito privacy.
Registri	X	Registro Titolare al trattamento Dati personali Registro Formazione Protocollo di studio
Procedure	X	Documents and Data Management Plan Istruzioni per lo Sperimentatore

Politiche di tutela della privacy	X	FTLS ha nominato un DPO e all'interno dell'Azienda esiste un Gruppo aziendale Privacy, che ha il compito di garantire e coordinare le attività aziendali correlate alla normativa in materia di protezione dei dati personali, supportando il Titolare del trattamento negli adempimenti previsti dalla normativa (Regolamento EU 2016/679, Decreto Legislativo 196/2003 e s.m.i.).
Misure anti – intrusive (cartelli di divieto di accesso ai locali, strumenti per la rilevazione degli accessi, guardiania, portineria, serrature armadi, schedari, ecc.)	x	La sicurezza fisica dei locali della FTLS è garantita da sistemi di videosorveglianza, controllo degli accessi da parte del personale della sicurezza (presente 24 ore su 24, 7 giorni su 7). Inoltre, i locali dove vengono effettuati i trattamenti più sensibili sono accessibil dal solo personale autorizzato mediante badge identificativo. I documenti sono inoltre conservati in armadi chiusi a chiave in locali con accesso controllato. Al TMF hanno accesso esclusivamente i membri del Team Studi Clinici.
Politiche di sicurezza informatica	X	Sulle postazioni aziendali viene garantito l'aggiornamento dei Sistemi Operativi e di un programma di antivirus e di anti-malware completo. Ogni dispositivo consegnato al dipendete ha disco criptato. I sistemi informatici sono configurati per eseguire autonomamente gli aggiornamenti di sicurezza. Tutti i dati sono protetti da misure di progettazione sicura dell'infrastruttura di rete e protezione dall'accesso non autorizzato alla rete.
Distruzione/smaltimento sicuro cartaceo	X	La distruzione della documentazione dopo il periodo previsto avverrà tramite trita documenti di tipo a particelle/frammenti almeno P4.
Inventario degli asset	X	Le postazioni di lavoro aziendali, come l'intera infrastruttura ICT, sono censite a cura dell'Amministratore di Sistema incaricato.
Controllo accessi (log)	x	Registrazione dei log di accesso al server, verifica dei log dall'Event Viewer di ciascuna postazione degli utenti abilitati come Amministratori di Sistema.
Antivirus / firewall	x	Presenti e con aggiornamenti automatici
Politiche di clear screen	X	Blocco automatico, utilizzo obbligatorio di credenziali sicure per riattivare lo schermo

Back – up dei dati	x	I sistemi informativi della FTLS sono soggetti a backup secondo le procedure ICT concordate con la Direzione
Pseudonimizzazione	x	Utilizzo di codici univoci per ciascun partecipante allo Studio. Solo il responsabile della ricerca o altri soggettida questi autorizzati, possono collegare i codici all'identità dei partecipanti.
Sicurezza dei documenti cartacei	X	I documenti cartacei vengono conservati dal personale designato che verifica che siano disposti in specifici raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi non autorizzati. I dati raccolti e conservati in armadi chiusi a chiave in stanze con accesso consentito solo a personale autorizzato.
Gestione postazioni	X	Le postazioni sono accessibili dai soli utenti aziendali. È presente un regolamento aziendale sull'utilizzo delle postazioni e dell'infrastruttura informatica.
Autenticazione	X	Access and password policy aziendale
Policy di gestione data breach	X	L'Azienda ha adottato una procedura di gestione delle violazioni dei dati personali in cui sono definite le modalità operative da seguire in caso di incidente. La medesima procedura viene fornita ai Responsabili del trattamento in quanto disciplina anche le violazioni esterne all'Azienda. È previsto un registro aziendale delle violazioni. Dipendenti edotti sulla procedura.
Policy di data retention	X	L'Azienda ha adottato una procedura di data retention, per gestire la conservazione dei dati personali secondo basi giuridiche chiare e tempistiche di conservazione e cancellazione coordinate e pre-definite.

14 Minacce

14.1 Accesso illegittimo ai dati

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

Diffusione dei dati non autorizzata

14.1.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato delle password di accesso ai pc aziendali; sottrazione delle password di accesso da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; virus; accesso non autorizzato all'archivio dei TMF.

14.1.3 Quali sono le fonti di rischio?

Fonti umane (personale addetto).
Fonti non umane (attacchi informatici e/o malfunzionamenti dei sistemi)

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

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti –intrusive; Politiche di sicurezza informatica; Controllo accessi (log); Antivirus/firewall; Politiche di trasmissione dei dati; Crittografia; Pseudonimizzazione; accesso a un numero limitato di addetti (principio Need to know); Team interno dedicato alla supervisione delle attività legate alla conduzione dello studio presso il Promotore.

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

Bassa: l'impatto sugli interessati potrebbe essere elevato presso il Centro, presso lo Sponsor non vi è possibilità di attribuire il codice pseudonimizzato al paziente incluso nello studio. Nessun dato personale in chiaro degli stessi è presente nei sistemi informatici né nel materiale cartaceo presente in FTLS. Le misure previste per evitare gli accessi non autorizzati rendono limitata la probabilità di accadimento.

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

Molto bassa: le politiche di sicurezza informatica e le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento.
FTLS ritiene di aver implementato misure tecniche idonee a prevenire il rischio derivante da fonti di rischio umane interne (Gestione del personale mediante autorizzazione al trattamento e fornitura di istruzioni), esterne (Gestione dei terzi che accedono ai dati mediante la sottoscrizione di data protection agreement contenente specifiche istruzioni volte ad innalzare il livello di sicurezza) e non umane (quali controllo degli accessi logici, gestione vulnerabilità, antivirus, sicurezza canali informatici, crittografia, access management, protezione perimetrale della rete, segregazione di rete).

14.2 Modifiche indesiderate dei dati

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

Perdita di integrità del dato; la modifica potrebbe essere definitiva e avere conseguenze sulla qualità dei risultati dello studio.

14.2.2 Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo inappropriato delle password di accesso ai pc aziendali; sottrazione delle password di da parte di un terzo; operatori abilitati che sfruttano i privilegi di accesso per accedere illegittimamente alle informazioni; attacco informatico; errata profilazione degli utenti; virus; accesso non autorizzato all'archivio delle cartelle TMF.

14.2.3 Quali sono le fonti di rischio?

Fonti umane interne (lasciare incustodita la postazione di lavoro, alterazione volontaria di dati, errore umano involontario).
Fonti non umane (attacchi informatici e/o malfunzionamenti dei sistemi)

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

Istruzioni persone autorizzate trattamento; Formazione; Procedure; Politiche di tutela della privacy; Misure anti –intrusive; Politiche di sicurezza informatica; Controllo accessi (log); antivirus/firewall; Back – up dei dati; Team interno dedicato alla supervisione delle attività legate alla conduzione dello studio presso il Promotore.

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

Bassa: le misure adottate a protezione delle postazioni di lavoro e della conservazione della documentazione riducono notevolmente la probabilità di accadimento.

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

Molto bassa: le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimento. La conservazione dei documenti contenenti dati personali e/o particolari avviene in archivi ad accesso riservato e controllato.

14.3 Perdita dei dati

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

Una perdita dei dati potrebbe causare l'alterazione dei risultati dello Studio o la impossibilità di proseguire lo Studio; tuttavia, non si tratta di dati originali presso lo Sponsor.

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

La minaccia principale è quella di una distruzione o cancellazione erronea o volontaria dei dati. Le principali minacce possono essere di natura informatica (infezione da ransomware provocando anche solo in modo temporaneo una impossibilità ad accedere all'infrastruttura aziendale, guasto che determina il danneggiamento, l'interruzione o la non disponibilità del sistemai) o derivare da una azione umana (utilizzo improprio della posta elettronica da parte di un operatore attraverso cui un virus potrebbe bloccare il sistema aziendale; Incidente tecnico/ambientale alla sala server, fattori ambientali quali incendi o allagamenti ai locali dedicati alla conservazione dei TMF)

14.3.3 Quali sono le fonti di rischio?

Fonti umane interne (operatori autorizzati che abusino del proprio ruolo o colposamente operino cancellazioni sui dati per inesperienza o imperizia; lasciare incustodita la postazione di lavoro; lasciare incustodite sulla scrivania le cartelle TMF dello Studio);
Fonti non umane (attacchi informatici e/o malfunzionamenti dei sistemi, blocchi attività server room)

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

Back – up dei dati; Controllo accessi (log); Misure anti – intrusive; sistema antincendio, antivirus/firewall; Tracciabilità, Gestione postazioni; Politiche di tutela della privacy¸ Politiche di sicurezza informatica.

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

Molto bassa: i dati non sono originali, quindi l'impatto sugli interessati non è elevato, inoltre le misure previste per evitare la perdita dei dati rendono limitata la probabilità che essa si verifichi.

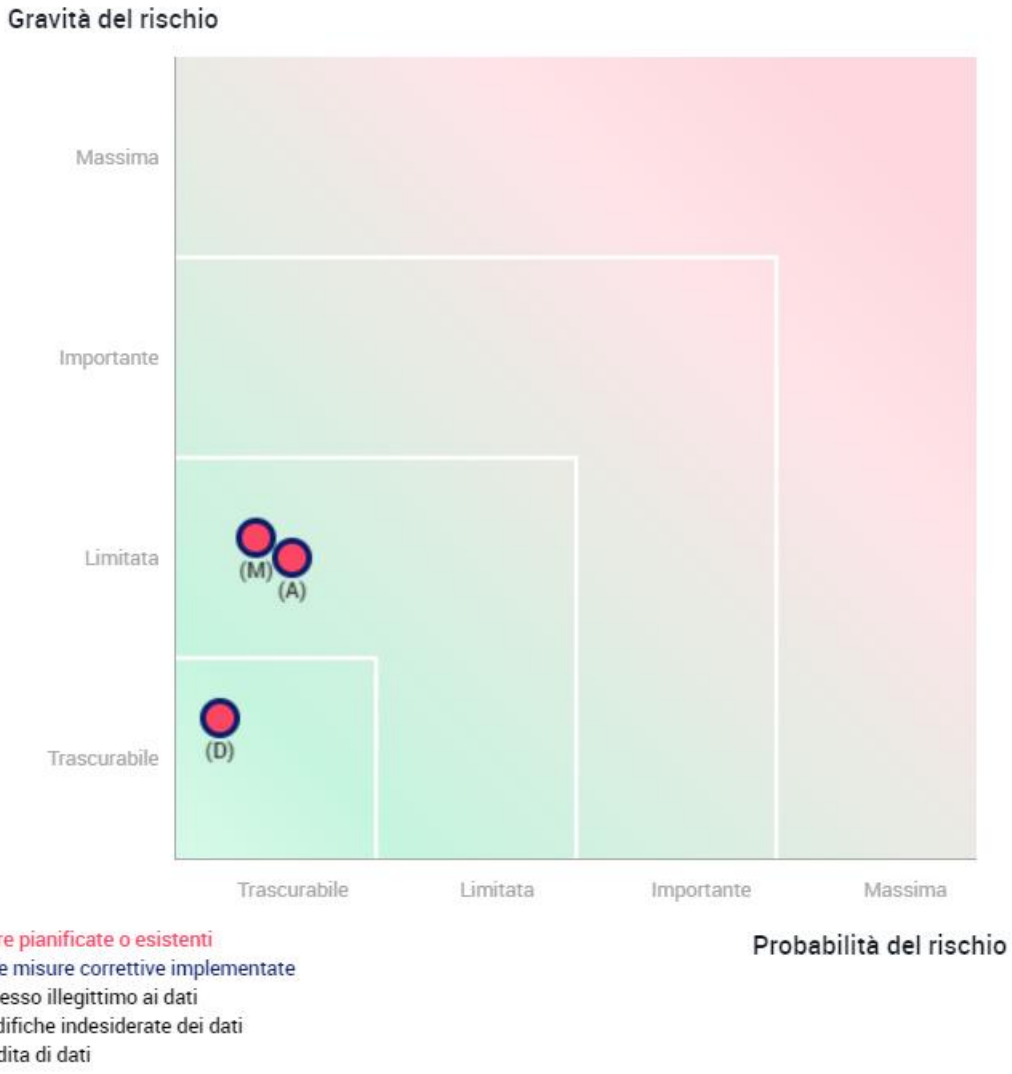
14.3.6 Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Molto bassa: le misure adottate a protezione delle postazioni di lavoro e degli archivi cartacei rendono quasi nulla la probabilità di accadimenti. FTLS ritiene di aver implementato misure

tecniche idonee a prevenire il rischio derivante da fonti di rischio umane interne (Gestione del personale mediante autorizzazione al trattamento e fornitura di istruzioni), esterne (Gestione dei terzi che accedono ai dati mediante la sottoscrizione di data protection agreement contenente specifiche istruzioni volte ad innalzare il livello di sicurezza) e non umane (quali controllo degli accessi logici, gestione vulnerabilità, antivirus, sicurezza canali informatici, crittografia, access management, protezione perimetrale della rete, segregazione di rete, impianto antincendio e procedure dedicate).

FTLS ha adottato una procedura per la gestione dei data breach e una procedura per la gestione dell'esercizio dei diritti degli interessati all'interno della sua organizzazione.

15 Valutazione del Rischio



Tenuto conto della natura, del contesto, delle finalità, dell'ambito di applicazione del trattamento in esame e delle misure adottate, il livello di rischio residuo, considerato accettabile indicato dal Titolare, sentito anche il parere del DPO, è risultato BASSO.

***

Il Titolare del trattamento, in persona del direttore Generale Procuratore, preso atto delle valutazioni sopra riportate in ordine all'analisi del potenziale impatto per i diritti e le libertà degli interessati autorizza affinché il documento:

a) sia reso pubblico sul sito internet istituzionale del Centro nell'apposita sezione;

b) sia resa disponibile agli interessati, su istanza dei medesimi.

Andrea Paolini
10.02.2026 09:15:40
GMT+01:00

Data..... Firma del Direttore Generale.....