REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

VALUTAZIONE DI IMPATTO DEL TRATTAMENTO - DPIA

STUDIO CLINICO OSSERVAZIONALE RETROSPETTIVO

“Studio osservazionale, retrospettivo, multicentrico sulla valutazione delle caratteristiche clinico-strumentali e di follow-up dei pazienti affetti da Plasmocitoma solitario Multifocale (Studio MULTIPLAS)”

Redazione	Unità per la ricerca clinica (URC)
Valutazione	Ufficio Privacy
Validazione	DPO

CONTESTO

PANORAMICA DEL TRATTAMENTO

Quale è il trattamento in considerazione?

La presente valutazione d'impatto prende in considerazione lo studio osservazionale retrospettivo, multicentrico, nazionale “Studio osservazionale, retrospettivo, multicentrico sulla valutazione delle caratteristiche clinico-strumentali e di follow-up dei pazienti affetti da Plasmocitoma solitario Multifocale (Studio MULTIPLAS)".
La finalità dello studio è di tipo non commerciale (no profit).
Lo studio si propone di valutare le informazioni riguardanti la presentazione clinica, le caratteristiche di esordio e di evoluzione dei pazienti affetti da Plasmocitoma solitario Multifocale e degli *outcome* in relazione alle terapie a cui sono stati sottoposti nei vari centri, al di fuori di trial clinici sponsorizzati “*real-world*”. Tale proposta rappresenta la prima raccolta di questa peculiare tipologia di pazienti ed i risultati attesi potrebbero chiarire l’entità della casistica e allo stesso tempo, fornire informazioni esplorative di tipo prognostico-predittivo, utili per l’identificazione di protocolli terapeutici più adeguati a questa categoria di pazienti.

L'obiettivo primario dello studio è la caratterizzazione e presentazione clinica delle caratteristiche del Plasmocitoma Solitario Multifocale.
L'obiettivo secondario è:
- Stabilire se la prognosi è differente rispetto ai pazienti con diagnosi di Mieloma multiplo sintomatico (IMWG).

L'obiettivo esplorativo è:
- Verificare la sopravvivenza globale, *progression free-survival* in relazione ai protocolli terapeutici utilizzati nei vari Centri partecipanti.

Quali sono le responsabilità connesse al trattamento?

Il Promotore I.R.C.C.S. Istituto Tumori “Giovanni Paolo II” di Bari è titolare del trattamento dei dati. Presso l’I.R.C.C.S. lo Sperimentatore principale è il Dott. Bernardo Rossini, Dirigente Medico Ematologo presso l’U.O.C. Ematologia e Terapia Cellulare.

L’Azienda ULSS n. 2 Marca trevigiana è centro partecipante alla ricerca ed è coinvolto in qualità di autonomo titolare del trattamento dei dati.
Lo studio si svolgerà presso la UOC Ematologia dell'Azienda ULSS n. 2 Marca trevigiana. Presso il centro lo Sperimentatore principale è la Dr.ssa Anna Furlan.

Ci sono standard applicabili al trattamento?

Non ci sono allo stato standard applicabili al trattamento.

DATI, PROCESSI E RISORSE DI SUPPORTO

Quali sono i dati trattati?

I dati raccolti saranno dati identificativi (dati anagrafici e di contatto) e categorie particolari di dati di cui all'art. 9 GDPR, quali: dati relativi alla salute, con specifico riferimento ai dati molecolari afferibili alle analisi condotte sul materiale biologico e ai dati relativi alla neoplasia ottenuti durante il percorso diagnostico. Nello specifico da Talete e dalle cartelle cliniche cartacee ambulatoriali dei pazienti verranno raccolti i seguenti dati:

- nome
- cognome
- sesso
- data di nascita

Da Talete e dalle cartelle cliniche cartacee ambulatoriali verranno, altresì, raccolti i dati relativi alla salute di seguito riportati:

- ECOG performance status, data della diagnosi, ISS, R-ISS, R2-ISS (quest'ultima se disponibile), caratteristiche cellulari del midollo osseo (fenotipo e biopsia osteomidollare), esame FISH (se disponibile);
- numero e tipo di localizzazioni scheletriche (almeno uno dei segmenti scheletrici coinvolti sottoposto ad accertamento istologico con evidenza di infiltrato plasmacellulare);
- imaging delle localizzazioni scheletriche (TAC, RMN, PET), elettroforesi con immunofissazione sierica e urinaria per valutare la proteina monoclonale coinvolta e il relativo livello sierico e urinario, free light chain;
- dosaggio delle immunoglobuline, immunoparesi, emoglobina, globuli bianchi, piastrine, calcemia, PCR, VES, LDH, Beta2microglobulina, albumina, proteinuria delle 24 ore e velocità di filtrazione glomerulare (eGFR), plasmocitoma solitario all'esordio, radioterapia, tempo alla progressione, esecuzione BOM alla progressione, coinvolgimento sedi ossee alla progressione, lesione d'esordio sede di progressione, biopsia su altra sede ossea, data inizio e tipologia di trattamento di prima linea e numero di cicli effettuati, linee successive di trattamento alla ricaduta, eleggibilità al trapianto autologo di cellule staminali e data del trapianto, tossicità ematologica ed extraematologica, *outcome* clinico (data e stato ultimo follow-up).

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il ciclo di vita del dato ha origine dall'acquisizione dei dati relativi alla salute dalla cartella clinica del paziente i quali vengono, poi, riportati dallo sperimentatore nella CRF elettronica crittografata con password.

I dati relativi all'identità dei pazienti sono sottoposti a pseudonimizzazione eseguita secondo le indicazioni riportate nello specifico paragrafo indicato nelle misure di sicurezza in essere. Tali dati sono trasferiti in forma pseudonimizzata al Promotore con gli strumenti di condivisione concordati con lo stesso.

Presso l'Unità Operativa Ematologia, sotto la responsabilità dello sperimentatore principale, in un file separato (tabella di transcodifica) saranno conservate le associazioni codice pseudonimizzato (generatore casuale) e nome/cognome del paziente.
I dati sono analizzati per il tempo strettamente necessario alla conduzione dello studio (24 mesi), al termine del quale saranno conservati per un periodo massimo di dieci anni, come indicato nell'informativa privacy da fornire al paziente ed eventualmente trattati, previa anonimizzazione, per finalità di pubblicazione scientifica e per convegni/seminari.

Quali sono le risorse di supporto ai dati?
Per il supporto alla raccolta dei dati dello studio sono utilizzati:

- CRF elettronica
- Software aziendale per la gestione dei dati clinici (TALETE)
- Cartelle cliniche cartacee ambulatoriali

PRINCIPI FONDAMENTALI

PROPORZIONALITÀ E NECESSITÀ

Gli scopi del trattamento sono specifici, espliciti e legittimi?
I dati sono trattati per finalità di ricerca scientifica e raccolti in base agli obiettivi specifici descritti nel protocollo di studio approvato dal competente Comitato Etico. Il soggetto partecipante allo studio riceve una informativa che descrive nel dettaglio le caratteristiche dello studio e i dati che saranno raccolti, nonché un modulo per esprimere il consenso informato per la partecipazione allo studio. Viene, inoltre, sottoposta al paziente l'informativa per il trattamento dei dati personali, unitamente al relativo modulo di consenso.
Tutta la modulistica firmata in originale viene conservata presso l'Unità Operativa Ematologia che sarà responsabile del reclutamento dei pazienti.

Quali sono le basi legali che rendono lecito il trattamento?
La base giuridica è il consenso dell'interessato:

- dati di natura comune: art. 6, par. 1, lettera a) del GDPR;
- dati particolari: art. 9, par. 2, lettera a) del GDPR.

Presso il centro è previsto l'arruolamento di due pazienti di cui uno in vita e uno deceduto.
Il paziente in vita sarà contattato telefonicamente per fornire le informazioni relative a obiettivi e caratteristiche dello studio.
Si procederà a contattare lo stesso recuperando i dati di contatto dall'anagrafe degli assistiti e si terrà quindi un registro dei tentativi di contatto: il paziente verrà ritenuto non contattabile solo dopo 3 tentativi documentati.

Ai pazienti raggiungibili verrà sottoposto il modulo di consenso informato per lo studio, approvato dal Comitato Etico, di cui riceverà una copia. Il rilascio del consenso informato sarà registrato nella cartella del paziente.
È prevista l'inclusione nello studio di un paziente deceduto. La verifica del decesso verrà effettuata attraverso anagrafe sanitaria regionale, dopo l'approvazione del Comitato Etico Territoriale.
In considerazione della tipologia e rarità della patologia e del ristretto numero di casi seguiti presso il centro, la mancata considerazione dei dati del paziente deceduto produrrebbe conseguenze significative per lo studio in termini di alterazione dei relativi risultati compromettendo il conseguimento delle finalità della ricerca.
Ai sensi degli artt. 6, par. 1, lettera e), 9, par. 2, lettera j) e art. 89 del GDPR, in combinato disposto con l'art. 110, comma 1, del D.Lgs. n. 196/2003, nonché del Provvedimento del Garante per la protezione dei dati personali del 09.05.2024, il trattamento dei dati dei pazienti deceduti e di quelli non contattabili richiede, oltre all'approvazione del Comitato Etico, l'effettuazione e la pubblicazione della valutazione di impatto, dandone comunicazione al Garante per la protezione dei dati personali.

Resta fermo l'obbligo di rendere l'informativa agli interessati inclusi nello Studio in tutti i casi in cui, nel corso dello stesso, ciò sia possibile e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento.

Al fine di garantire la massima trasparenza e tutelare i diritti di tutti i pazienti non raggiungibili per i motivi sopra indicati e degli aventi causa del paziente deceduto il Promotore pubblicherà sul proprio sito istituzionale la valutazione di impatto predisposta per lo studio, nonché l'informativa per il trattamento dei dati personali.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?
I dati, compresa la scheda di raccolta dati, sono raccolti e trattati secondo quanto indicato nel protocollo di studio, valutato e approvato dal Comitato Etico competente. I dati sono successivamente analizzati secondo quanto definito nel piano di analisi del protocollo. In base al principio di minimizzazione, sono trattati esclusivamente i dati necessari per le finalità dello studio.

I dati sono esatti e aggiornati?
Sono utilizzati dati già raccolti nell'ambito dell'assistenza clinica. Non è previsto un aggiornamento o una verifica di quanto già raccolto.

Qual è il periodo di conservazione dei dati?
Lo studio ha una durata di 24 mesi dall'approvazione dello stesso. A seguito della sua conclusione, i dati saranno conservati per dieci anni e successivamente distrutti. I dati potrebbero essere trattati poi in forma aggregata e anonima per eventuali pubblicazioni scientifiche o convegni/seminari.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Come sono informati del trattamento gli interessati?

Il soggetto che partecipa allo studio riceve, al primo contatto utile, sia l'informativa relativa allo studio sia quella relativa al trattamento dei dati personali. Copia della predetta documentazione è altresì pubblicata nel sito internet aziendale, nella specifica sezione dedicata alla ricerca.
Essendoci un paziente deceduto, viene altresì applicato l'art. 110, comma 1, del D.Lgs. n. 196/2003, in base al quale i dati dei pazienti deceduti e di quelli non contattabili saranno trattati solo dopo l'approvazione del Comitato Etico e la comunicazione al Garante per la protezione dei dati personali.
Resta fermo l'obbligo di rendere l'informativa agli interessati inclusi nello Studio in tutti i casi in cui, nel corso dello stesso, ciò sia possibile e, in particolare, laddove questi si rivolgano al centro di cura, anche per visite di controllo, anche al fine di consentire loro di esercitare i diritti previsti dal Regolamento.

Ove applicabile: come si ottiene il consenso degli interessati?

I pazienti saranno contattati telefonicamente per fornire le informazioni relative a obiettivi e caratteristiche dello studio, recuperando i dati di contatto dall'anagrafe sanitaria regionale.
Nel caso di accesso del paziente in Azienda ULSS n. 2 per visita o controllo di routine, verrà presentata dal medico responsabile la specifica informativa dello studio. Si lascia il tempo sufficiente al soggetto per leggere con attenzione la documentazione. Nell'ambito della stessa visita o nella successiva si procede alla raccolta dei consensi firmati.
Per particolari esigenze legate alla tipologia di studio e di pazienti, la raccolta del consenso potrà avvenire in modalità telematica, mediante raccolta dello stesso da parte del medico sperimentatore a seguito di condivisione dei documenti con e-mail e ricezione dei documenti firmati con allegata la carta di identità del firmatario, trasmessi in modalità sicura (documenti cifrati e accessibili tramite una password per l'apertura del file consegnata separatamente all'interessato, in base a quanto previsto dal DPCM 8 agosto 2013).

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Secondo quanto previsto dal Regolamento aziendale concernente la protezione dei dati personali, viene garantito l'esercizio dei diritti di cui al presente paragrafo anche attraverso la specifica modulistica pubblicata. Per assicurare che i dati vengano resi disponibili soltanto al legittimo proprietario, prima di procedere con l'evasione di una richiesta, viene attentamente verificata l'identità dell'interessato. Nel sito internet aziendale, al link https://www.aulss2.veneto.it/privacy , è prevista la specifica modulistica per l'esercizio dei diritti. L'interessato potrà esercitare i diritti rivolgendosi o al promotore, eventualmente anche per tramite dello sperimentatore, o al centro di sperimentazione, tramite i recapiti indicati nell'informativa.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
Secondo quanto previsto dal regolamento aziendale concernente la protezione dei dati personali, viene garantito l'esercizio dei diritti di cui al presente paragrafo anche attraverso la specifica modulistica pubblicata. Per assicurare che i dati vengano resi disponibili soltanto al legittimo proprietario, prima di procedere con l'evasione di una richiesta, viene attentamente verificata l'identità dell'interessato. Nel sito internet aziendale, al link https://www.aulss2.veneto.it/privacy , è prevista la specifica modulistica per l'esercizio dei diritti. L'interessato potrà esercitare i diritti rivolgendosi o al promotore, eventualmente anche per tramite dello sperimentatore, o al centro di sperimentazione, tramite i recapiti indicati nell'informativa. Il diritto alla cancellazione non è applicabile per i dati clinici di partenza.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
Secondo quanto previsto dal Regolamento aziendale concernente la protezione dei dati personali, viene garantito l'esercizio dei diritti di cui al presente paragrafo anche attraverso la specifica modulistica pubblicata. Per assicurare che i dati vengano resi disponibili soltanto al legittimo proprietario, prima di procedere con l'evasione di una richiesta, viene attentamente verificata l'identità dell'interessato. Nel sito internet aziendale, al link https://www.aulss2.veneto.it/privacy , è prevista la specifica modulistica per l'esercizio dei diritti. L'interessato potrà esercitare i diritti rivolgendosi o al promotore, eventualmente anche per tramite dello sperimentatore, o al centro di sperimentazione, tramite i recapiti indicati nell'informativa.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?
L'Azienda ULSS n. 2 per la conduzione di questo studio non si avvale di un soggetto esterno per specifiche attività (per esempio per l'analisi statistica, o per l'esecuzione di attività di laboratorio), e, pertanto, non viene predisposta una specifica nomina a Responsabile del trattamento dati.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?
Non è previsto il trasferimento verso Paesi Extra UE.

RISCHI

MISURE ESISTENTI O PIANIFICATE

Controllo degli accessi logici
Gli accessi in dominio sono concessi dal servizio di ICT, a seguito di richiesta scritta e firmata da parte del Direttore dell'Unità Operativa Ematologia.
Le richieste includono:

- generalità del richiedente;
- natura del rapporto con l'Azienda (dipendente o altro);
- date di inizio/fine del rapporto con l'Azienda.

Il servizio abilitazioni vaglia ogni singola abilitazione, scartando quelle incoerenti o inappropriate. L'accesso alle aree di share è consentito secondo le policy aziendali, in relazione all'unità operativa di appartenenza.
Lo Sperimentatore principale condividerà la documentazione prodotta con i soli appartenenti allo staff dello studio.
La documentazione cartacea riguarda i dati del progetto e pochi limitati dati personali, essendo questi trattati principalmente in modalità informatizzata.
La documentazione viene conservata in armadi all'interno delle Unità Operative coinvolte nella gestione dello studio, accessibile solo dal personale autorizzato, secondo le tempistiche indicate all'interno del protocollo di ricerca approvato dal competente Comitato Etico. Una volta terminata la fase di arruolamento dei pazienti, tutta la documentazione sarà conservata presso la l'Unità Operativa Ematologia.

Minimizzazione dei dati
Il protocollo approvato dal Comitato Etico stabilisce sia il set di informazioni cui si può accedere, sia il *dataset* di informazioni che devono essere poi successivamente raccolte, catalogate e valutate, oltre anche all'arco temporale di analisi. L'accesso ai dati clinici è consentito solamente al personale medico, mentre al restante personale (ricercatori), è consentito il trattamento dei soli dati necessari all'attività di ricerca prevista dal singolo progetto.

Gestione delle postazioni
Le postazioni utilizzate sono in dominio aziendale e le misure adottate sono quelle previste da regolamenti e *policy* aziendali. I dispositivi esterni e personali non ottengono l'accesso all'*intranet* aziendale se non tramite la VPN precedentemente abilitata.

Sicurezza dei siti web
Il Promotore non carica le informazioni su portali web di proprietà.

Sicurezza dei canali informatici
L'*intranet* è protetta da sistemi di *firewall* aziendale: gli unici dispositivi autorizzati a poter aprire canali di comunicazione nell'*intranet* aziendale sono quelli preventivamente registrati e autorizzati (solamente dispositivi aziendali). Qualora sia richiesta l'abilitazione per un dispositivo personale, questa viene attentamente vagliata, e prima di procedere alla connessione viene adeguato secondo lo standard di *policy* aziendale (es. antivirus aziendale).

Controllo degli accessi fisici
L'accesso ai locali è consentito unicamente al personale autorizzato.

Politica di tutela della privacy
Il titolare ha nominato un RPD. Il Titolare - da atto aziendale - ha individuato uno specifico servizio (ufficio privacy) incardinato nell'UOC Affari Generali. Il Titolare ha adottato uno specifico "Regolamento concernente la protezione dei dati personali", periodicamente revisionato, disponibile su sito *web* aziendale e condiviso con tutto il personale.

Gestione del personale
Il personale riceve, all'atto dell'assunzione o con specifica comunicazione, la nomina ad autorizzato o delegato al trattamento, con le relative istruzioni operative. All'atto dell'avvio del progetto, lo sperimentatore principale è individuato quale delegato al trattamento: vengono, inoltre, individuati i soggetti autorizzati alla partecipazione al progetto.

Lotta contro il *malware*
Tutte le postazioni e i dispositivi aziendali sono equipaggiati con *antivirus* e *anti-malware* aziendale.

Gestione delle politiche di tutela della privacy
Il Titolare effettua degli *audit* periodici in ordine al rispetto del Regolamento aziendale sulla protezione dei dati personali e della diversa regolamentazione aziendale che abbia un impatto sul trattamento dati e realizza percorsi formativi *ad hoc* per tutto il personale, sia generali che specifici per determinati ambiti di trattamento.

Gestione degli incidenti di sicurezza e delle violazioni dei dati personali
Il titolare si è dotato di specifica procedura per la gestione dei *data breach*. L *'incident response plan* è in corso di valutazione da parte della Direzione.

Sicurezza dell'hardware
L'accesso avviene da postazioni con sistema operativo aggiornato con le ultime release di sicurezza approvate dai Sistemi Informativi.

Sicurezza dei documenti cartacei
È onere di ogni singolo soggetto coinvolto nello specifico progetto di ricerca, condividere la documentazione prodotta con i soli appartenenti all'equipe di ricerca.
Normalmente la documentazione cartacea riguarda i dati del progetto e pochi limitati dati personali, essendo questi trattati principalmente in modalità informatizzata.
Gli uffici dispongono di armadi con chiusura a chiave, accessibili solo dal personale autorizzato.

Tracciabilità
L'accesso ai gestionali informatici e alle cartelle di rete è tracciato da log, accessibili esclusivamente all'amministratore di sistema.

Pseudonimizzazione
I dati personali necessari per la conduzione dello studio vengono registrati in forma pseudonimizzata.
Il personale medico e autorizzato del Centro di riferimento provvede, infatti, a sostituire il nominativo dell'Interessato con un codice secondo un processo chiamato "pseudonimizzazione" (vedasi linee guida ENISA). Soltanto il medico sperimentatore e il personale autorizzato del centro possiede il codice (la chiave di decrittazione) che, se necessario, può essere utilizzato per ricollegare i dati pseudonimizzati al nominativo dell'Interessato, come in caso di visita di controllo, ispezione o audit. Altresì, i dati (*raw data*) che devono essere pubblicati su specifiche piattaforme, secondo le indicazioni del Ministero, sono resi disponibili in forma pseudonimizzata.

Backup
Secondo policy aziendali, i documenti che vengono memorizzati su specifiche aree di share aziendali sono oggetto di backup. La stessa politica viene adottata per i dati memorizzati su procedure aziendali. Per il dettaglio, si rimanda a quanto documentato e disponibile su intranet aziendale.

ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
- Perdita di riservatezza
- divulgazione dei dati
- danno all'immagine o alla dignità del soggetto interessato

Quali sono le principali minacce che potrebbero concretizzare il rischio?
- Comportamento improprio del personale interno
- utilizzo improprio di dispositivi non aziendali
- accesso abusivo esterno

Quali sono le fonti di rischio?
- Perdita dei dati
- perdita di dispositivi affidati a personale interno
- accesso a sistemi aziendali da parte di soggetti non autorizzati
- attacco ai sistemi aziendali
- autorizzazione errata su dispositivi e sistemi aziendali

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Controllo degli accessi logici
- minimizzazione dei dati
- gestione delle postazioni
- sicurezza dei canali informatici
- controllo degli accessi fisici
- politica di tutela della privacy
- gestione del personale
- lotta contro il malware
- gestione delle politiche di tutela della privacy
- sicurezza dell'hardware
- gestione degli incidenti di sicurezza e delle violazioni dei dati personali
- tracciabilità
- sicurezza dei documenti cartacei
- pseudonimizzazione

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

Trascurabile	**Limitato**	**Importante**	**Massimo**

L'accesso indesiderato ai dati di ricerca (non ai dati clinici dai quali si parte), determina la perdita di riservatezza su dati sanitari - rilevati ai fini dello studio - relativi ai pazienti coinvolti nello studio. La gravità è attenuata, dal momento che la catalogazione avviene con dati parzialmente aggregati o pseudonimizzati.

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

Trascurabile	**Limitato**	**Importante**	**Massimo**

Alla luce dei sistemi e procedure in essere, la probabilità di accadimento di un accesso illegittimo può essere ritenuta trascurabile perché:

- dati e documenti sono conservati e gestiti solamente su sistemi aziendali;
- i dispositivi che accedono all'*intranet* aziendale sono forniti o controllati direttamente dall'UOC Sistemi Informativi.
- Inoltre, al fine di diminuire ulteriormente la probabilità di accadimento del rischio, si procede a:
- una continua revisione delle *policy* aziendali per l'utilizzo del sistema informatico aziendale;
- una valutazione e verifica periodica sulla sicurezza dei sistemi aziendali;
- una adeguata formazione al personale sull'utilizzo degli strumenti aziendali (*hardware* e *software*);

- un adeguamento dei protocolli adottati per ciascun progetto di ricerca, che tenga conto dei principi di minimizzazione, *privacy by default* e *privacy by design*.

MODIFICHE INDESIDERATE DEI DATI

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

- Perdita di integrità dei dati oggetti di studio.

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

- Comportamento improprio del personale interno
- accesso abusivo esterno
- utilizzo improprio di dispositivi non aziendali

Quali sono le fonti di rischio?

- Attacco ai sistemi aziendali
- accesso a sistemi aziendali da parte di soggetti non autorizzati
- autorizzazione errata su dispositivi e sistemi aziendali
- perdita di dispositivi affidati a personale interno

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

- Controllo degli accessi logici
- gestione delle postazioni
- gestione del personale
- controllo degli accessi fisici
- politica di tutela della privacy
- lotta contro il malware
- gestione delle politiche di tutela della privacy
- gestione degli incidenti di sicurezza e delle violazioni dei dati personali
- sicurezza dei canali informatici
- sicurezza dell'hardware
- pseudonimizzazione
- backup

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

Trascurabile	**Limitato**	**Importante**	**Massimo**

La gravità del rischio, nel caso di perdita dei dati oggetto di studio (non dei dati clinici dai quali si parte), ai fini dei diritti e le libertà delle persone fisiche può essere considerato trascurabile. Il rischio in analisi (perdita di integrità) eventualmente impatta sulla

pubblicazione della ricerca e non tanto sui dati personali oggetto di trattamento; in ogni caso l'attività può essere ripresa, partendo dai dati clinici iniziali.

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

Trascurabile	**Limitato**	**Importante**	**Massimo**

Alla luce dei sistemi e procedure in essere, la perdita dei dati può ritenersi trascurabile in quanto l'accesso ai dati è regolamentato e profilato. In ogni caso la perdita potrebbe riguardare soltanto i singoli dati oggetto della ricerca.

PERDITA DI DATI

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

- Perdita di disponibilità dei dati oggetto di studio.

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

- Comportamento improprio del personale interno
- accesso abusivo esterno
- utilizzo improprio di dispositivi non aziendali

Quali sono le fonti di rischio?

- Attacco ai sistemi aziendali
- autorizzazione errata su dispositivi e sistemi aziendali
- perdita di dispositivi affidati a personale interno
- accesso a sistemi aziendali da parte di soggetti non autorizzati

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

- Controllo degli accessi logici
- gestione delle postazioni
- gestione del personale
- controllo degli accessi fisici
- politica di tutela della privacy
- lotta contro il malware
- gestione delle politiche di tutela della privacy
- gestione degli incidenti di sicurezza e delle violazioni dei dati personali
- sicurezza dei canali informatici
- sicurezza dell'hardware
- pseudonimizzazione
- backup

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

Trascurabile	**Limitato**	**Importante**	**Massimo**

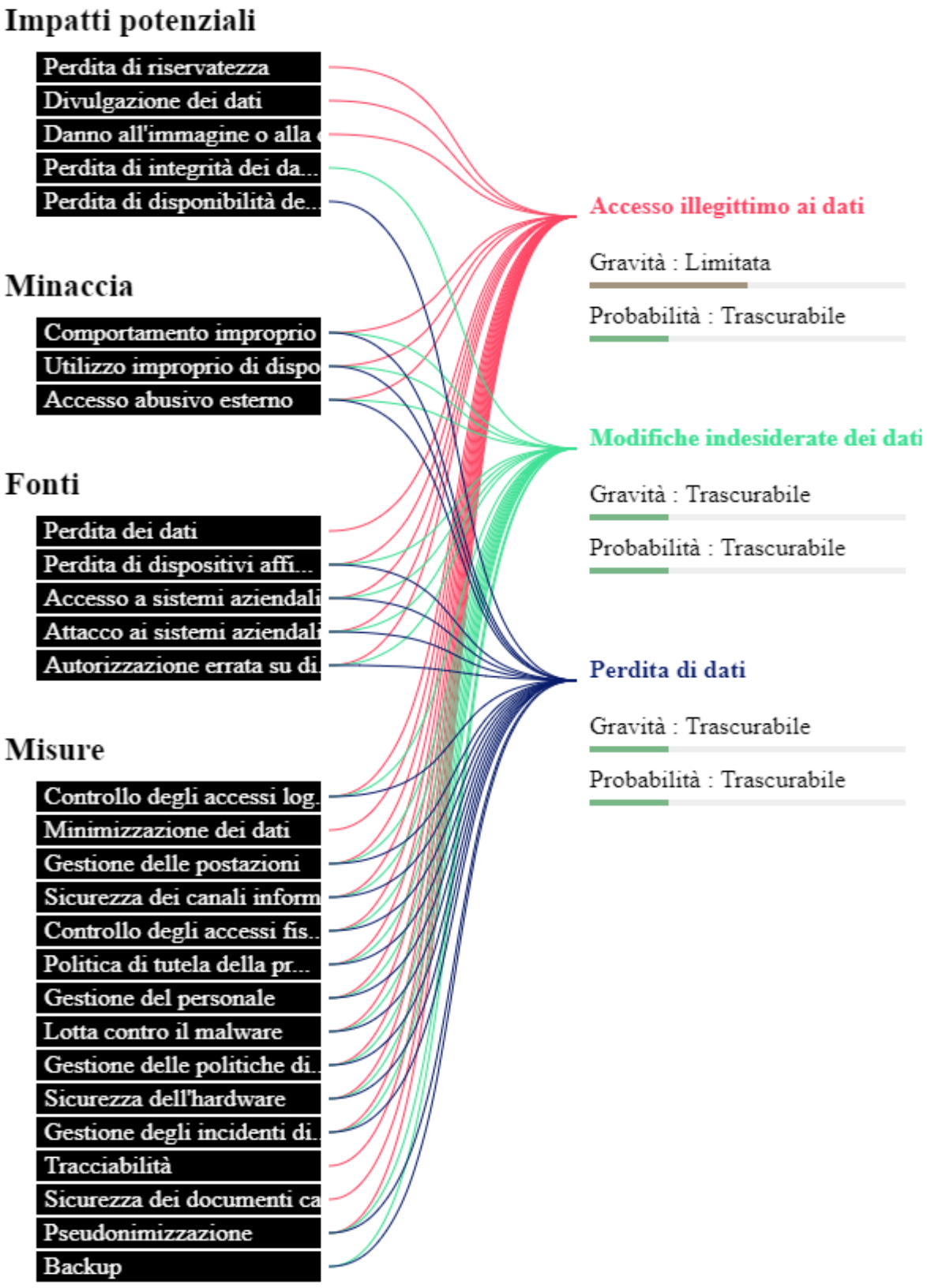
La gravità del rischio, nel caso di perdita dei dati oggetto di studio (non dei dati clinici dai quali si parte), ai fini dei diritti e le libertà delle persone fisiche può essere considerato trascurabile. Il rischio in analisi (perdita del dato) eventualmente impatta sulla pubblicazione della ricerca e non tanto sui dati personali oggetto di trattamento; in ogni caso l'attività può essere ripresa, partendo dai dati clinici iniziali.

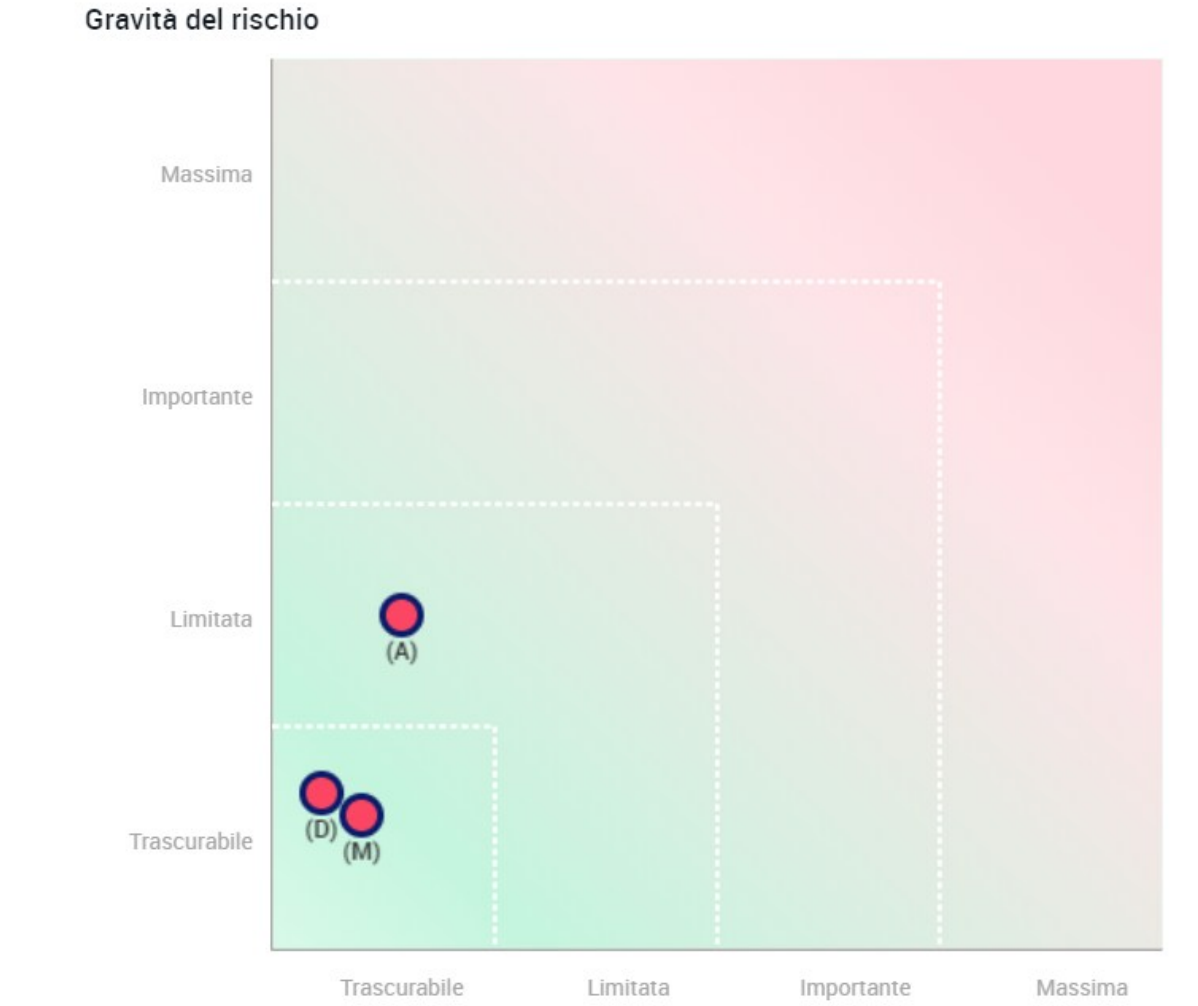
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile	**Limitato**	**Importante**	**Massimo**

Alla luce dei sistemi e procedure in essere, la perdita dei dati può ritenersi trascurabile in quanto l'accesso ai dati è regolamentato e profilato. In ogni caso la perdita potrebbe riguardare soltanto i singoli dati oggetto della ricerca.

PANORAMICA DEI RISCHI





- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

23/10/25

Valutazione complessiva: accettabile.

Treviso, 10 aprile 2026

Parere del DPO

A seguito della valutazione sul testo proposto, dei chiarimenti forniti da parte del servizio che ha redatto la DPIA e dell'analisi della documentazione e delle misure previste per lo studio oggetto di questa DPIA, si esprime una valutazione complessivamente positiva sulla conformità del trattamento ai requisiti del GDPR.
Le finalità specificate risultano proporzionate ai dati raccolti, sono state dichiarate idonee misure di sicurezza, e sono state esplicitate responsabilità e flussi di trattamento.

Il rischio residuo è valutato come trascurabile, a condizione che le misure individuate siano applicate e monitorate lungo l'intero svolgi

21/05/2026 09:28:54
DAMIANO NESO

Per il Titolare del trattamento

Azienda ULSS n. 2 Marca trevigiana
Il Direttore Generale
Dr. Giancarlo Bizzarri

BIZZARRI
GIANCARLO
27.05.2026
11:08:02
GMT+02:00