DPIA – Studio MOBO-REAL PI Pasello

Nome del DPO/RPD

RPD IOV Cristina Canella

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Vista la natura retrospettiva degli studi che sono condotti in seguito all'erogazione delle prestazioni di cura, data le misure di minimizzazione, di archiviazione, di sicurezza dei canali informatici, delle politiche di tutela della privacy, delle poltiche di gestione degli incidenti di sicurezza e violazione dei dati personali il rischio di perdita del controllo dei dati e della violazione della riservatezza residuo risulta limitato.

Richiesta del parere degli interessati

Non è richiesto il consenso degli interessati in quanto lo studio prevede la raccolta dei dati personali in maniera retrospettiva. I dati sono già presenti nei sistemi del titolare del trattamento e raccolti in occasione delle prestazioni sanitarie.
A tale riguardo poiché numerosi pazienti sono deceduti o risultati non reperibili, non essendo possibile informarli e raccogliere il relativo consenso si farà ricorso alle procedure dell'Art 110 del D. Lgs. 196/2003 e nel rispetto di quanto previsto dall'art. 89 GDPR.

Motivazione della mancata richiesta del parere degli interessati

Vista la natura retrospettiva degli studi che sono condotti in seguito all'erogazione delle prestazioni di cura, data le misure di minimizzazione, di archiviazione, di sicurezza dei canali informatici, delle politiche di tutela della privacy, delle poltiche di gestione degli incidenti di sicurezza e violazione dei dati personali il rischio di perdita del controllo dei dati e della violazione della riservatezza residuo risulta limitato

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

L'Istituto Oncologico Veneto è stato istituito con L.R. 22 dicembre 2005 n.26 ed è stato riconosciuto Istituto di Ricovero e Cura a Carattere ai sensi del d.lgs.288/2003, con DM 04.08.2023.
Pertanto, l'Istituto svolge, nella disciplina dell'oncologia, attività di prevalente ricerca biomedica e sanitaria e di assistenza sanitaria di tipo clinico e traslazionale.
Centrale per l'Istituto è l'attività di ricerca scientifica, perseguito nell'ambito dell'oncologia secondo standard di eccellenza.

In linea con la normativa regionale nazionale, IOV svolge attività di studio e di ricerca, trasferendo i dati validati nei processi assistenziali del Sistema Sanitario Regionale.
La presente valutazione rientra nel quadro di specifici progetti di ricerca, ovvero studi osservazionali retrospettivi, con promotore diverso da IOV, che rientrano anche nell'ambito dei programmi di ricerca biomedica o sanitaria previsti ai sensi dell'articolo 12-bis del Dlgs 30 dicembre 1992 n. 502).

Lo studio trattato nella presente valutazione d'impatto è lo studio MOBO-REAL promosso dall'Azienda Ospedale Universitaria Careggi che coinvolge tutte le Unità Oncologiche italiane che arruolano i pazienti nel Programma di richiesta del paziente individuale-IPRP con mobocertinib e che danno disponibilità alla partecipazione alla raccolta dati.
Trattasi di studio osservazionale, retrospettivo e prospettico, che arruola pazienti eleggibili con NSCLC avanzato precedentemente trattati che presentino l'inserzione dell'esone 20 di EGFR.

Quali sono le responsabilità connesse al trattamento?

In relazione al presente studio il Promotore e l'Istituto agiscono in qualità di autonomi titolari del trattamento, in seguito alle valutazioni fatte congiuntamente in sede di approvazione del protocollo di studio.
Il PI dello studio è nominato con atto di delega formale a firma del Direttore Generale ai sensi dell'art. 2-quaterdecies Codice Privacy come delegato del trattamento.

Ci sono standard applicabili al trattamento?

- Prescrizioni e delle Regole deontologiche, che costituiscono condizione essenziale di liceità e correttezza dei trattamenti (art. 2-quater del Codice e art. 21, comma 5, del d.lgs. 10 agosto 2018, n. 101).
- **Chiarimenti sull'applicazione della disciplina** per il trattamento **dei** dati relativi alla salute in ambito **sanitario** - **7 marzo 2019** [9091942]
- Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21 comma 1 del d.lgs. 10 agosto 2018 n. 101

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati raccolti includeranno:
- dati demografici (DOB, sesso, età alla diagnosi, stato di fumatore)
- dati clinico-patologici (PS ECOG alla diagnosi, istologia, tipo EGFR di inserzione dell'esone 20, espressione di PD-L1 e altre eventuali co-mutazioni)
- stadiazione con TAC torace, addome bacino e cervello se acquisito, stadiazione TNM alla diagnosi, sede della metastasi. Non è prevista acquisizione di immagini radiologiche

o metaboliche.
- trattamenti (trattamento precedente: tipo/durata e tipo di risposta, motivo dell'interruzione)
- trattamento con mobocertinib (data di inizio/fine, risposta clinica maggiore, eventuale riduzione della dose, dati sull'interruzione PD/tossicità/altro)
tossicità durante mobocertinib (tipo, grado, data di insorgenza, data di risoluzione dell'AE, eventuale riduzione del dosaggio, dati sulla sospensione della tossicità)
- valutazione clinica ad ogni visita (segni vitali, ECOG PS, tollerabilità, esami del sangue, AE)
- valutazione radiologica ogni 12 settimane circa (TC torace, addome bacino e cervello se clinicamente richiesto)
- follow-up di sopravvivenza (morte/ultimo f-up)

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

I dati vengono estrapolati dal sistema cartelle aziendale Galileo/Oncosys che sono consultabili tramite accesso con credenziali personali o SPID. L'accesso con credenziali è vincolato al personale medico di ruolo assunto da IOV facente parte del gruppo di sperimentazione.
Registrazione: I dati sono trasferiti e registrati sul portale RedCap al link https://rialab.dss.unifi.it/index.php?action=passwordreset&u=Z2FtYmFsZV9lbGlzYWJldHRh&k=5d838038ca5ae38f4ee51482208bdd06f2d2559966820632eede67bc2446ae4dc9272abbacea0fe4bcb74a2d81b35307b1a5bc903f372d10e069931c00c8644b con accesso vincolato da user e password temporanei in possesso dei soli medici che vengono abilitati all'accesso per il singolo database.
La base dati è organizzata in 9 sezioni
(Demographics, Medical/surgery History, Histology and baseline characteristics, previous cancer treatment, concomitant medical log, mobocertinib exposure as collected, instrumental re-evaluation, adverse event, end of treatment/study form).
Ogni sezione ha alcuni campi dove inserire il dato con vincolo relativo alla tipologia di dato inserito (p.e. data format, scelte
vincolate per inserimento di alcuni dati per ridurre il fattore errore, riconoscibilità del dato e omogeneizzare il più possibile il dato stesso). La piattaforma genera un codice identificativo univoco associato ad ogni soggetto coinvolto nello Studio, che consente ai ricercatori di mantenere localmente l'associazione con i rispettivi dati anagrafici.
La possibilità di risalire all'origine dei dati è giustificata dalla necessità di effettuare studi di follow up per i pazienti in cura presso le Unità Operative coinvolte.
conservazione: dove sono conservati i dati? I dati acquisiti vengono conservati all'interno del suddetto data base per tutta la durata dello studio.
Modifica: ogni singolo centro tramite credenziali personali attivate una per PI e una subinvestigator, può accedere ai propri dati per visionarli e/o modificarli.
estrazione: come avviene l'estrazione dei dati? I dati vengono estrapolati mediante apposita funzione presente su RedCap e denominata "data export tool" che permette, dopo attribuzione di un codice identificativo univoco randomico, di esportare tutti i dati o effettuare una selezione di quelli di interesse nella modalità di fruizione per l'analisi. Nel caso specifico verrà usato l'importatore nel software di analisi statistica denominato "R".
I dati sono accessibili con modalità unica attraverso
credenziali e password personale per ogni Data Entry Person. L'accesso alla visualizzazione dei dati pseudo-anonimizzati dipende dai privilegi che vengono assegnati dal Principal Investigator (PI) al momento della registrazione allo studio sul portale REDCap.
Pertanto, ogni

singolo centro può accedere ai propri dati per visionarli e/o modificarli, mentre il centro coordinatore (AOU-Careggi) nella persona del PI può accedere mediante credenziali personali ai dati raccolti trasversalmente da tutti i centri.

Quali sono le risorse di supporto ai dati?

- Sistemi di gestione delle cartelle cliniche adottati a livello aziendale
- Sistema RedCap
- Campioni biologici

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati sono trattati per finalità di ricerca scientifica. L'Istituto Oncologico Veneto, avendo qualifica di IRCCS, persegue legittimamente finalità di ricerca scientifica in ambito oncologico, stante il D.M. 6.6.2017 e la legge regionale 26/2005 di istituzione dell'Istituto. Le finalità sono rese esplicite perché dichiarate nelle informative e nei documenti predisposti per la ricerca scientifica.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Dati di natura comune: art. 6 par. I lettera e) Dati particolari: art. 9 par. II lettera j), in combinato disposto con l'art. 89 GDRP e art. 110 comma 1 prima parte D.Lgs. 196/2003.

Valutazione : Accettabile

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

I dati raccolti seguono un protocollo di ricerca che ne definisce gli obiettivi e il disegno, vengono utilizzati soltanto i dati relativi ai campioni pertinenti con il perimetro dello studio. Nel protocollo sono definiti in maniera precisa i criteri di inclusione o esclusione dallo studio, pertanto vengono inclusi soltanto i dati che corrispondono al profilo ricercato.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Per loro natura, per tali progetti nei protocolli non è prevista una fase di riverifica sulla correttezza dei dati che poi vengono analizzati. Una ulteriore revisione dei dati di partenza, viene invece effettuata a fronte di successivi progetti di ricerca, pertanto la revisione del dato di partenza (dato clinico) ha effetti solamente su eventuali nuovi studi e non anche su quelli già conclusi.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati saranno conservati per un periodo di almeno 7 anni, a termine del quale Alla fine dello studio, il Coordinatore dello studio distruggerà tale file eliminando tutti i legami tra i partecipanti allo studio, i dati e i campioni raccolti durante la ricerca dei pazienti inseriti nello studio.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Nelle informative affisse nei principali luoghi di transito e disponibile nel sito web istituzionale, è esplicito il riferimento all'attività di ricerca scientifica svolta dall'Istituto. Per questi specifici studi osservazionali, non è previsto il rilascio dell'informativa direttamente ai soggetti coinvolti nel progetto di ricerca, ma una specifica informativa è pubblicata - unitamente alla presente valutazione d'impatto - nella sezione privacy del sito istituzionale.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non è richiesto il consenso degli interessati in quanto lo studio prevede la raccolta dei dati personali in maniera retrospettiva. I dati sono già presenti nei sistemi del titolare del trattamento e raccolti in occasione delle prestazioni sanitarie.
A tale riguardo poiché numerosi pazienti sono deceduti o risultati non reperibili, non essendo possibile informarli e raccogliere il relativo consenso si farà ricorso alle procedure dell'Art 110 del D. Lgs. 196/2003.

Valutazione : Accettabile

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

Gli interessati possono esercitare il diritto di accesso:
• scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy dell'Istituto, reperibile sia nell'informativa generale che nel sito web istituzionale;
• direttamente presso il P.I. e la sua equipe (ciò avviene più frequentemente rispetto all'utilizzo della posta elettronica). Il diritto alla portabilità non è applicabile per tale attività di trattamento.

L'istituto ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Gli interessati possono esercitare il diritto di rettifica e di cancellazione - limitatamente a quanto applicabile:
• scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy dell'Istituto, reperibile sia nell'informativa generale che nel sito web istituzionale;
• manifestando la propria volontà direttamente al P.I. e alla sua equipe. L'istituto ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Gli interessati possono esercitare il diritto di opposizione e limitazione:
• scrivendo all'indirizzo di posta elettronica dedicato dell'Ufficio Privacy dell'Istituto, reperibile sia nell'informativa generale che nel sito web istituzionale;
• manifestando la propria volontà direttamente al P.I. e alla sua equipe.
L'istituto ha redatto una specifica procedura che definisce il comportamento da adottare internamente, all'atto di presentazione di un'istanza da parte degli interessati.

Valutazione : Accettabile

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

Per questa tipologia di trattamenti, non sono previsti responsabili esterni del trattamento.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Per questo studio non è previsto il trasferimento dei dati personali al di fuori dello Spazio Economico Europeo.

Valutazione : Accettabile

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 di Unità Operativa (ovvero direttamente dall'ufficio risorse umane per il personale contrattualizzato) presentata direttamente dal singolo interessato.
Le richieste includono:
• generalità del richiedente
• natura del rapporto con l'Istituto Oncologico Veneto (dipendente o altro) date di inizio/fine del rapporto con l'Istituto Oncologico Veneto
• 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'U.O. di appartenenza.
L'accesso alle aree condivise viene autorizzato dal P.I. che coordina il progetto di ricerca.

Valutazione : Accettabile

Archiviazione

I CFR dei pazienti verranno generati e gestiti tramite piattaforma RedCap in utilizzo presso il Promotore. Il sistema RedCap è protetto da un protocollo crittografico conforme allo standard PGP.

Valutazione : Accettabile

Tracciabilità

Il sistema RedCap è dotato di un sistema di registrazione dei log.

Valutazione : Accettabile

Minimizzazione dei dati

Il protocollo condiviso e autorizzato con il Comitato Etico stabilisce sia il set di informazioni cui si può accedere, sia o il dataset di informazioni che devono essere poi successivamente raccolte, catalogate e valutate, oltre anche all'arco temporale di analisi.
Il personale di ricerca si impegna a non trattare dati eccedenti e ridondanti rispetto alle finalità perseguite.

Valutazione : Accettabile

Lotta contro il malware

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

Valutazione : Accettabile

Backup

Secondo policy aziendali, i documenti che vengono memorizzati su specifiche aree di share aziendali sono oggetto di backup da parte del personale di ricerca. Stessa politica viene adottata per i dati memorizzati su procedure aziendali.
Inoltre per la natura retrospettiva dei dati che vengono estratti dalla cartella clinica, una copia degli stessi è sempre reperibile dalla consultazione della cartella clinica digitale.

Valutazione : Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

L'Istituto ha adottato e ha reso nota una apposita procedura per la gestione degli eventi potenzialmente qualificabili come data breach che delinea in maniera chiara i ruoli e le responsabilità in casi di sospetta violazione dei dati personali.

Valutazione : Accettabile

Pseudonimizzazione

I dati vengono sottoposti ad una procedura di pseudonimizzazione tramite l'assegnazione di un codice alfa numerico randomico che individua: - nella prima parte del codice il centro partecipante - nella seconda il paziente arruolato.
Il promotore non è tenuto a conoscere l'identità del paziente, la cui conoscenza è nell'esclusiva disponibilità del personale coinvolto nella ricerca di ogni singolo centro partecipante.

Valutazione : Accettabile

Crittografia

Il Promotore garantisce l'adozione di specifiche tecniche crittografiche che rendano inintellegibili i dati a soggetti estranei allo studio oggetto della presente valutazione d'impatto.
Il sistema RedCap prevede la crittografia dei dati, che sono conservati su storage S3 crittografato sulla piattaforma Amazon AWS, Cluster di Milano.

Valutazione : Accettabile
Commento di valutazione :
Date le misure di minimizzazione, di pseudonimizzazione, di critttografia, backup, controllo degli accessi logici, di sicurezza dei canali informatici, e data la natura retrospettiva degli studi che prende dati comunque archiviati in altre forme come la cartella clinica informatizzata, il rischio di eventuale perdita dei dati residuale rimane limitata.

Politica di tutela della privacy

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. Il titolare ha nominato un RPD.
Il Titolare - da atto aziendale - ha individuato uno specifico servizio (ufficio privacy) incardinato nell'U.O. Affari Generali.

Valutazione : Accettabile

Gestione del personale

Il personale viene adeguatamente formato in merito alle attività di trattamento e ai sistemi di sicurezza da adottare.
Per tale scopo:
• sono redatti specifici regolamenti interni
• vengono effettuate sessioni formative
• vengono effettuati audit presso le strutture interessate

Valutazione : Accettabile

Sicurezza dell'hardware

L'intranet è protetta da sistemi di firewall aziendale in gestione ad AOPD: 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)

Valutazione : Accettabile

Integrare la protezione della privacy nei progetti

L'Istituto, conformemente alla disciplina del Reg. (UE) 2016/679, gestisce i dati nel rispetto del principio di privacy per impostazione predefinita e per disegno. I dati trattati sono soltanto quelli strettamente necessari per le finalità perseguite, in ossequio al principio di minimizzazione.
Lo IOV lavora in maniera continua sull'utilizzo delle più aggiornate tecniche di anonimizzazione e pseudonimizzazione, in modo da tutelare la privacy dei soggetti arruolati nei progetti di ricerca.
Lo IOV ha redatto e diffuso un manuale per l'adozione di tecniche di anonimizzazione e pseudonimizzazione e mette a disposizione dei ricercatori il supporto di personale dei sistemi informativi specializzato nell'utilizzo del software adottato dall'istituto.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

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

Rischio di reidentificazione, Perdita di riservatezza, Perdita di controllo sull'utilizzo dei dati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Utilizzo improprio dei dispositivi aziendali, Perdita delle credenziali di accesso agli applicativi, Sottrazione delle credenziali di accesso

Quali sono le fonti di rischio?

Attacchi al sistema informativo aziendale, Perdita di dispostivo aziendale

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale

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

Limitata, Limitata, Data la natura retrospettiva degli studi che sono condotti in seguito all'erogazione delle prestazioni di cura, data le misure di minimizzazione, di pseudonimizzazione il rischio di perdita del controllo dei dati e della riservatezza residuo risulta limitato anche se si raccomanda di porre molta attenzione al processo di pseudonimizzazione e alle tecniche di crittografia in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale accesso illegittimo.

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

Limitata, Limitata, Date le misure di minimizzazione, di pseudonimizzazione, date le politiche privacy, la politica degli accessi logici il rischio di perdita della riservatezza nonché risultano limitati anche se si raccomanda di porre molta attenzione al processo di pseudonimizzazione e alle tecniche di crittografia in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale accesso illegittimo.

Valutazione : Accettabile

Rischi

Modifiche indesiderate dei dati

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

Nessun impatto reale

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

Errata elaborazione dei dati, Errato inserimento dei dati

Quali sono le fonti di rischio?

Comportamento improprio del personale interno

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

Archiviazione, Minimizzazione dei dati, Backup, Tracciabilità, Politica di tutela della privacy, Gestione del personale

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

Trascurabile, Gli eventuali impatti di una modifica dei dati riguardano i risultati della ricerca e non gli interessati.

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

Trascurabile, Evento estremamente improbabile.

Valutazione : Accettabile

Rischi

Perdita di dati

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

Perdita di controllo sull'utilizzo dei dati, Perdita di riservatezza, Rischio di reidentificazione

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

Perdita delle credenziali di accesso agli applicativi, Sottrazione delle credenziali di accesso, Utilizzo improprio dei dispositivi aziendali

Quali sono le fonti di rischio?

Attacchi al sistema informativo aziendale, Comportamento improprio del personale interno, Perdita di dispostivo aziendale

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

Minimizzazione dei dati, Tracciabilità, Archiviazione, Politica di tutela della privacy, Integrare la protezione della privacy nei progetti, Sicurezza dell'hardware

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

Limitata, Data la natura retrospettiva degli studi che sono condotti in seguito all'erogazione delle prestazioni di cura, data le misure di minimizzazione, di archiviazione, di sicurezza dei canali informatici, delle politiche di tutela della privacy, delle poltiche di gestione degli incidenti di sicurezza e violazione dei dati personali il rischio di perdita del controllo dei dati e della riservatezza residuo risulta limitato anche se si raccomanda di porre molta attenzione alla formazione e gestione del personale, nonché alla corretta implementazione delle politiche della privacy e di minimizzazione in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale perdita di dati.

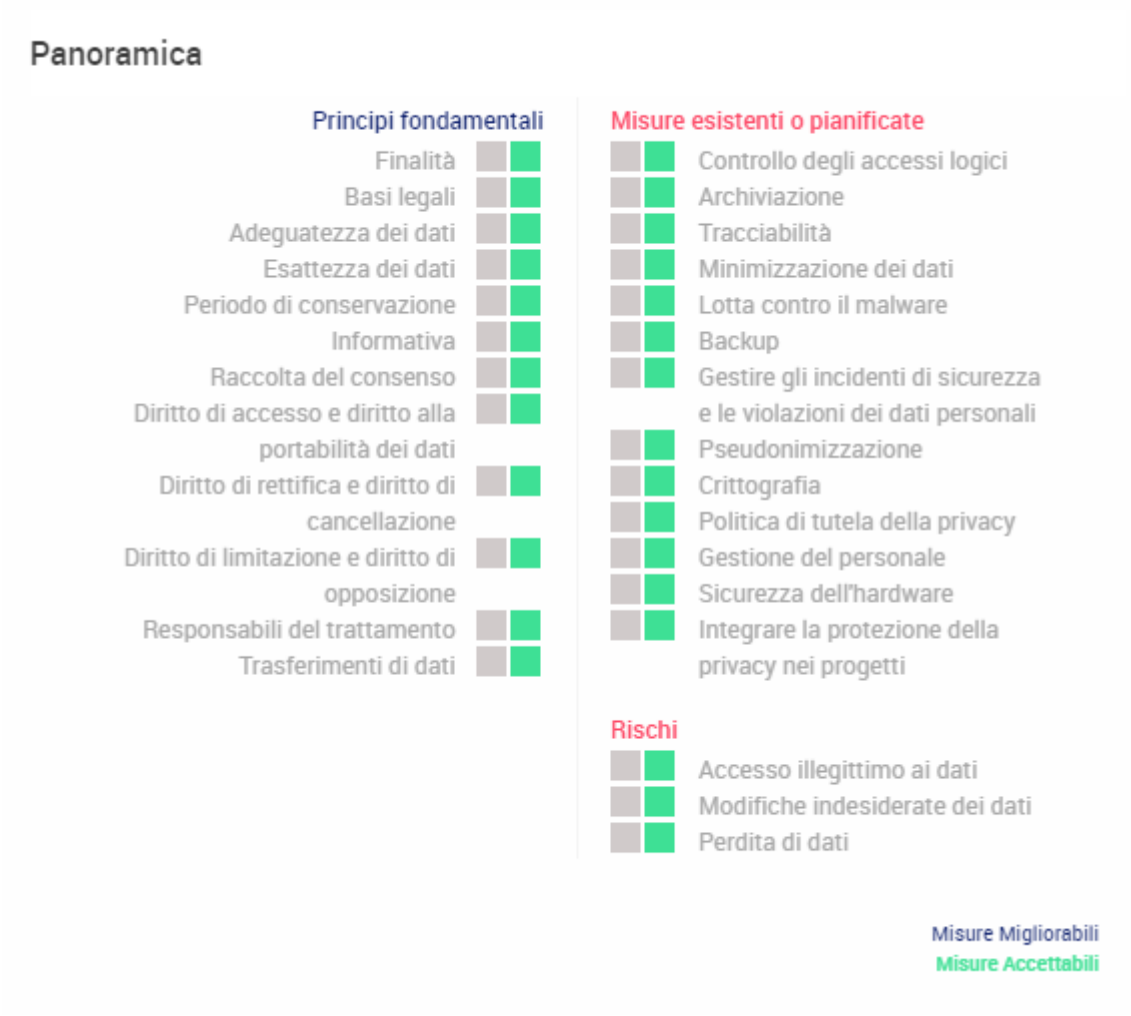
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Date le misure di minimizzazione, di pseudonimizzazione, di critttografia, backup, controllo degli accessi logici, di sicurezza dei canali informatici, e data la natura retrospettiva degli studi che prende dati comunque archiviati in altre forme come la cartella clinica informatizzata, il rischio di eventuale perdita dei dati residuale rimane limitata.

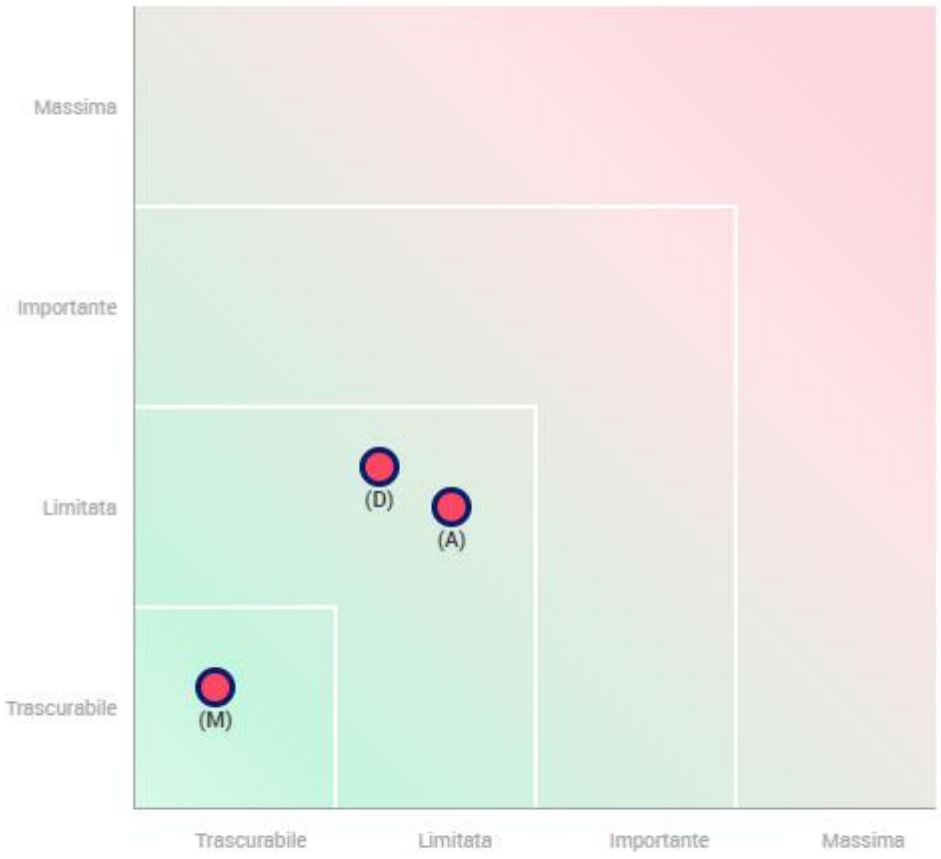
Valutazione : Accettabile

Rischi

Panoramica dei rischi

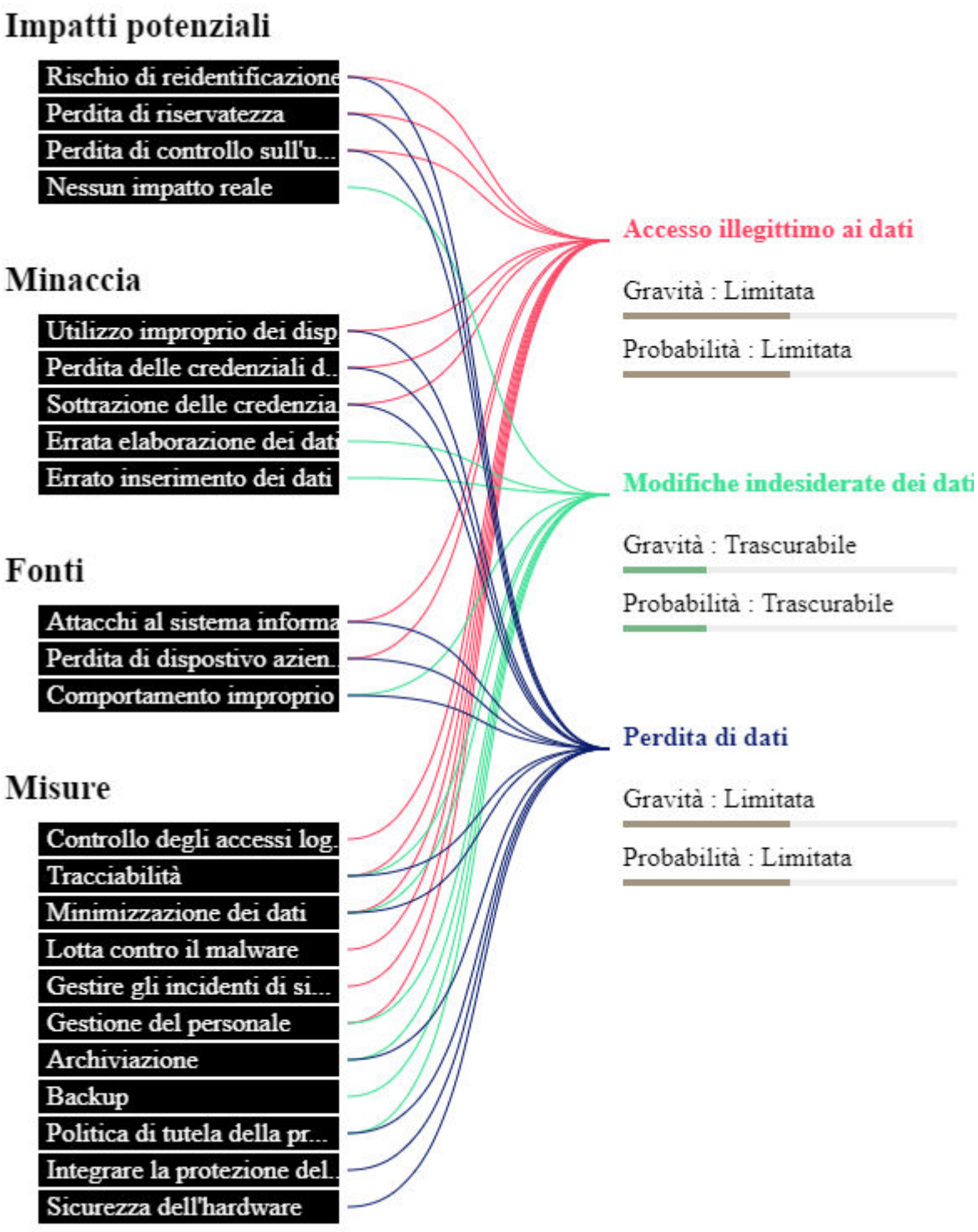


Gravità del rischio



Probabilità del rischio

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


Impatti potenziali
Rischio di reidentificazione
Perdita di riservatezza
Perdita di controllo sull'u...
Nessun impatto reale
Minaccia
Utilizzo improprio dei disp
Perdita delle credenziali d...
Sottrazione delle credenzia...
Errata elaborazione dei dati
Errato inserimento dei dati
Fonti
Attacchi al sistema informa...
Perdita di dispostivo azien...
Comportamento improprio
Misure
Controllo degli accessi log...
Tracciabilità
Minimizzazione dei dati
Lotta contro il malware
Gestire gli incidenti di si...
Gestione del personale
Archiviazione
Backup
Politica di tutela della pr...
Integrare la protezione del...
Sicurezza dell'hardware
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Limitata