DPIA – Studio osservazionale multicentrico IraBica PI Bergamo

Nome del DPO/RPD

DPO 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 politiche 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). Per tali progetti, lo IOV-IRCCS propone al Ministero della Salute un piano di studi triennale, strutturato in linee di ricerca, e ciascuna di queste declinata in una serie di progetti che poi vengono sviluppati durante il triennio (c.d. ricerca corrente).

La norma citata riguarda sia la ricerca finalizzata, che il Ministero promuove e finanzia di propria iniziativa.

Nella presente valutazione d'impatto l'oggetto è lo Studio multicentrico osservazionale retrospettivo denominato IraBica che prevede la raccolta di dati clinici di pazienti affetti da istotipi rari di neoplasie epiteliali delle vie biliari nell'arco temporale che intercorre dal primo gennaio 2002 al trentuno luglio 2022 ed è promosso dal Policlinico Universitario "G.Martino" di Messina.

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 trattati sono:
- dati di natura comune (anagrafici e di contatto);

- dati di natura particolare ex art. 9 GDPR (dati sulla salute, dati genetici)
I dati sono trattati esclusivamente in forma pseudonimizzata dal personale addetto alla ricerca, cioè dal personale sanitario specificamente individuato e autorizzato. Il Promotore dello studio non ha accesso ai dati dei pazienti arruolati "in chiaro" e riceve solo i dati pseudonimizzati.

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

I dati raccolti dai centri partecipanti verranno inseriti in RedCap in forma pseudonimizzata.
Eventuali pubblicazioni non tratteranno dati personali, in quanto gli stessi saranno preventivamente anonimizzati e soggetti a misure tecniche e organizzative finalizzate ad impedire la reidentificazione degli interssati.
Verrà condotta un'analisi di tipo statistico sulla base dei metadati estratti in formato xml da RedCap.

Quali sono le risorse di supporto ai dati?

Gli strumenti di raccolta ed elaborazione dei dati sono:
- Piattaforma REDCAP per la conservazione e condivisione dei CRF;
- Sistema informativo ospedaliero da cui si estraggono i dati delle cartelle cliniche;

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?

La conservazione avverrà per un periodo di 5 anni a decorrere dalla dati conclusione dello studio; al termine dei cinque anni i dati personali saranno anonimizzati definitivamente.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Sarà prodotta un'informativa da rendere agli interessati che li informi del trattamento dei dati oggetto della presente valutazione, in conformità al provvedimento del Garante della Privacy che autorizza questo studio.

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 e nel rispetto di quanto previsto dall'art. 89 GDPR.

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

Crittografia

I dati sono inseriti in un database SQL provvisto di crittografia.
I canali di comunicazione sono crittografati in SSL3 e https.

Valutazione : Accettabile

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

Tracciabilità

RedCap è provvisto di un tool di tracciamento delle attività svolte e degli accessi eseguiti.

Valutazione : Accettabile

Archiviazione

RedCap lavora su un database SQL in cloud su server localizzati all'interno dell'UE.

Valutazione : Accettabile

Backup

Viene effettuato un backup automatico del DB giornaliero con storicità pari a 7 giorni.

Valutazione : Accettabile

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

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

Gestione delle politiche di tutela della privacy

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

Anonimizzazione

Al termine del progetto e per la condivisione dei risultati, i dati vengono sottoposti ad anonimizzazione secondo le seguenti tecniche:

- ELIMINAZIONE dalla CRF e, conseguentemente, dal DB di alcuni parametri come, ad esempio, il Record ID e il Numero di centro;
- GENERALIZZAZIONE mediante aggregazione e K-anonimato di 12 variabili assicurando così che ogni valore relativo ad un soggetto interessato sia condiviso da almeno un numero minimo (K) di altre persone all'interno dell'insieme.

Pertanto, se ciò non avviene, si deve prevedere di aggregare i soggetti in gruppi che contengono almeno K soggetti.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

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

Perdita di confidenzialità, 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 della ricerca, Sottrazione delle credenziali di accesso agli applicativi in uso per la ricerca

Quali sono le fonti di rischio?

Comportamento improprio del personale, Attacchi al sistema informativo aziendale, Attacchi al sistema RedCap

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Backup, Integrare la protezione della privacy nei progetti, Gestione delle politiche di tutela della privacy

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 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,

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?

Errore nell'inserimento dei dati in RedCap, Errata elaborazione dei dati

Quali sono le fonti di rischio?

Comportamento improprio del personale

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Politica di tutela della privacy, Backup

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

Trascurabile, Non vi sono sostanziali impatti sugli interessati, l'eventuale errore nella compilazione delle CRF ha un effetto esclusivamente sulla qualità della ricerca.

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

Trascurabile, Evento altamente improbabile.

Valutazione : Accettabile

Rischi

Perdita di dati

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

Perdita di confidenzialità, Perdita di controllo sull'utilizzo dei dati, Perdita di riservatezza

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

Perdita delle credenziali di accesso agli applicativi della ricerca, Sottrazione delle credenziali di accesso agli applicativi in uso per la ricerca, Utilizzo improprio dei dispositivi aziendali, Perdita del dispositivo aziendale

Quali sono le fonti di rischio?

Attacchi al sistema RedCap, Attacchi al sistema informativo aziendale, Comportamento improprio del personale

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

Crittografia, Tracciabilità, Backup, Controllo degli accessi logici, Gestione delle politiche di tutela della privacy

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 politiche 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 crittografia, 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

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Diritto di accesso e diritto alla portabilità dei dati
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

Misure esistenti o pianificate

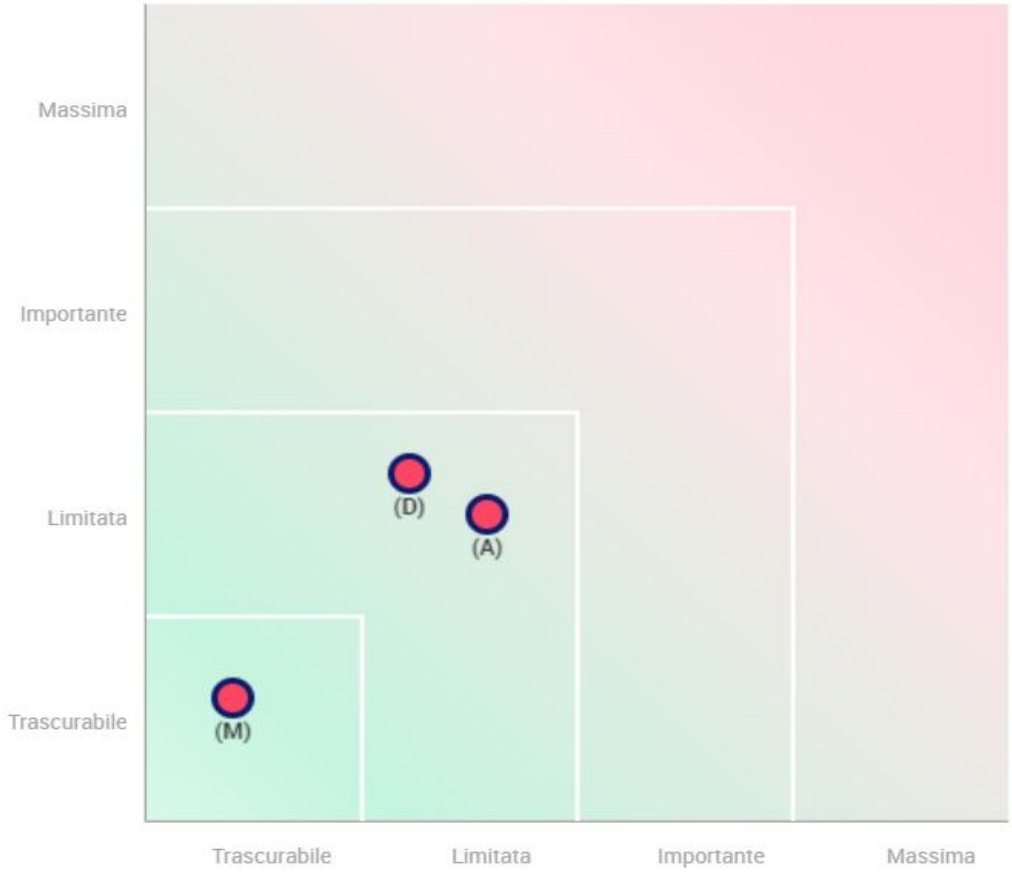
- Crittografia
- Controllo degli accessi logici
- Tracciabilità
- Archiviazione
- Backup
- Politica di tutela della privacy
- Integrare la protezione della privacy nei progetti
- Gestione delle politiche di tutela della privacy
- Anonimizzazione

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

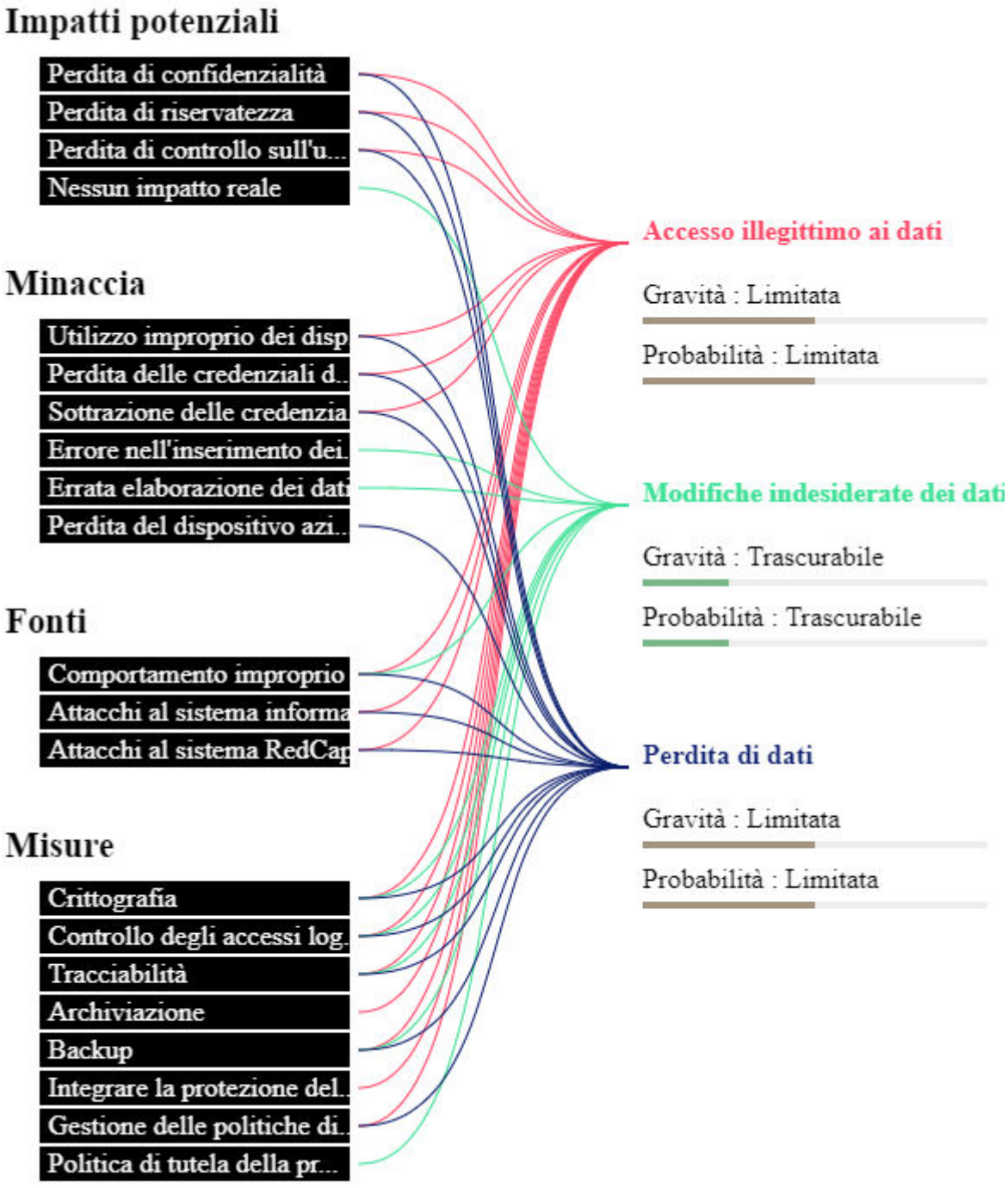
Misure Migliorabili
Misure Accettabili

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


Impatti potenziali
Perdita di confidenzialità
Perdita di riservatezza
Perdita di controllo sull'u...
Nessun impatto reale
Minaccia
Utilizzo improprio dei disp
Perdita delle credenziali d...
Sottrazione delle credenzia
Errore nell'inserimento dei
Errata elaborazione dei dati
Perdita del dispositivo azi...
Fonti
Comportamento improprio
Attacchi al sistema informa
Attacchi al sistema RedCap
Misure
Crittografia
Controllo degli accessi log...
Tracciabilità
Archiviazione
Backup
Integrare la protezione del...
Gestione delle politiche di...
Politica di tutela della pr...
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Limitata