
# Valutazione d'impatto sullo studio osservazionale multicentrico – TEBE AP

### Nome del DPO/RPD

DPO IOV dott.ssa 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 stato chiesto il parere degli interessati.

### Motivazione della mancata 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

# 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.

La presente valutazione d'impatto ha ad oggetto lo studio denominato TEAB-EAP, svolto in collaborazione con il Policlinico Gemelli IRCCS in qualità di Promotore, che ha come obiettivo primario quello di definire la sopravvivenza dei pazienti affetti da melanoma uveale in fase avanzata trattati con tebentafusp nell'ambito del programma di accesso allargato al farmaco.

All'interno dello IOV, saranno arruolati 5 pazienti.

### 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?

Per il presente studio saranno raccolte le seguenti categorie di dati:

- dati anagrafici (nome, caratteristiche demografiche
- dati sanitari (data della diagnosi; data dell'eventuale trattamento locoregionale per il tumore primitivo, data della diagnosi; - data dell'eventuale trattamento locoregionale per il tumore primitivo)
- dati biometrici (peso e altezza);

I dati, come di consueto nella ricerca clinica, saranno trattati solo in forma pseudonimizzata dal Promotore, che potrà verificare, conformemente alla buona pratica clinica, i dati della ricerca in chiaro tramite il proprio Monitor soltanto per il tempo strettamente necessario e *on site*.

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

I dati estratti dalle cartelle cliniche saranno trascritti su una CRF elettronica e sottoposto a procedura di pseudonimizzazione, vengono trasferiti al Promotore tramite mail, in allegato e con file criptato secondo standard PGP, con password comunicata in separata sede.
I dati verranno poi conservati per anni dopo la fine della ricerca per sette anni dopo il termine dello studio (previsto nella durata di 9 mesi) per finalità di verifica della qualità della ricerca, al termine del quale il Promotore provvederà alla loro distruzione.

### Quali sono le risorse di supporto ai dati?

- Email aziendale
- Cartella Clinica Elettronica
- Software di file automation
- Amnesya

**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 i), in combinato disposto con l'art. 89 GDRP e art. 110 comma 1 prima parte D.Lgs. 196/2003.
Il PI ha dichiarato l'impossibilità di raccogliere il consenso degli interessati in quanto deceduti e ha trasmesso questa attestazione al nucleo di ricerca clinica che l'ha messa agli atti.

**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 dal Promotore, per il tempo necessario allo svolgimento della ricerca clinica (9 mesi da protocollo di studi) e poi per un periodo non superiore a sette anni dal suo termine.

**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. Sul punto il PI ha compilato e sottoscritto un modulo, in uso presso l'istituto, per attestare le motivazioni che hanno reso impossibile la raccolta di tale consenso.

**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

Il file da inoltrare al Promotore viene preventivamente crittografato secondo lo standard PGP, con chiave di decriptazione trasferita in separata sede.

**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

Gli accessi alle cartelle cliniche elettroniche sono registrati in automatico con l'indicazione dell'orario, del giorno, dell'unità operativa e dell'operatore che vi ha avuto accesso.

**Valutazione : Accettabile**

## Archiviazione

I CFR dei pazienti verranno generati e gestiti tramite gli applicativi di software office automation, sono conservati su specifiche aree di share aziendale sotto la responsabilità del personale di ricerca.

**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. 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.

**Valutazione : Accettabile**

## Lotta contro il malware

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).

**Valutazione : Accettabile**

## Gestione postazioni

Le postazioni utilizzate sono principalmente in dominio aziendale e le misure adottate sono quelle previste da regolamenti e policy aziendali. I dispositivi esterni e personali non possono ottenere l'accesso all'intranet 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. In ogni caso i dati originali sono sempre disponibili in quanto conservati su sistema di gestione della cartella clinica elettronica.

**Valutazione : Accettabile**

## Sicurezza dei canali informatici

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**

## Controllo degli accessi fisici

L'accesso ai locali è bloccato da serrature con codice: il codice di accesso è rilasciato al solo personale che abbia necessità ad accedere a tali locali (anche se condivisi con altri professionisti), oltre al personale del servizio di pulizia.

**Valutazione : Accettabile**

## Politica di tutela della privacy

L'istituto è dotato di un regolamento sulla tutela dei dati personali che stabilisce in maniera chiara ruoli, regole e responsabilità per il trattamento dei dati personali all'interno dell'Istituto.

**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**

## 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**

## Gestione del personale

Il personale dell'istituto è debitamente formato con cadenza periodica sulla normativa in materia di protezione dei dati personali, con un focus specifico in funzione dei trattamenti svolti. Inoltre il personale all'atto dell'autorizzazione al trattamento dei dati personali ex art. 29 GDPR, riceve dal Titolare le istruzioni per il trattamento ed è messo a conoscenza delle procedure interne che disciplinano determinati trattamenti e che sono sempre consultabili tramite apposite aree del sistema informativo aziendale.
Inoltre: 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**

## 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**

## Vigilanza sulla protezione dei dati

L'Istituto ha nominato un responsabile della protezione dati, e rivede con cadenza periodico le procedure e le documentazioni prodotte in ossequio al Regolamento (UE) 679/2016.

**Valutazione : Accettabile**

# Rischi

# Accesso illegittimo ai dati

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

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

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

Perdita di dispositivo aziendale, Furto di dispositivo aziendale, Captazione del dataset oggetto di trasferimento

### Quali sono le fonti di rischio?

Virus informatico generico, Comportamento inappropriato del personale interno, Comportamento inappropriato del personale esterno, Attaccante esterno

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Lotta contro il malware, Gestione postazioni, Sicurezza dei canali informatici, Controllo degli accessi fisici, Vigilanza sulla protezione dei dati, Pseudonimizzazione, Gestire gli incidenti di sicurezza e le violazioni dei dati personali

### 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 limitare gli effetti negativi 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 di perdita di controllo sull'utilizzo dei dati 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 compilazione CRF, Errata elaborazione del dataset

### Quali sono le fonti di rischio?

Comportamento inappropriato del personale interno

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

Backup, Gestione del personale

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

Trascurabile, Trascurabile, un eventuale modifica indesiderata dei dati della ricerca avrebbe un impatto sul trial ma nessuno sugli interessati

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

Trascurabile, Molto 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?

Captazione del dataset oggetto di trasferimento, Furto di dispositivo aziendale, Perdita di dispositivo aziendale

## Quali sono le fonti di rischio?

Attaccante esterno, Comportamento inappropriato del personale esterno, Comportamento inappropriato del personale interno, Virus informatico generico, attaccante esterno

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

Crittografia, Controllo degli accessi logici, Minimizzazione dei dati, Gestione postazioni, Lotta contro il malware, Sicurezza dei canali informatici, Controllo degli accessi fisici, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Vigilanza sulla protezione dei dati

## 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.

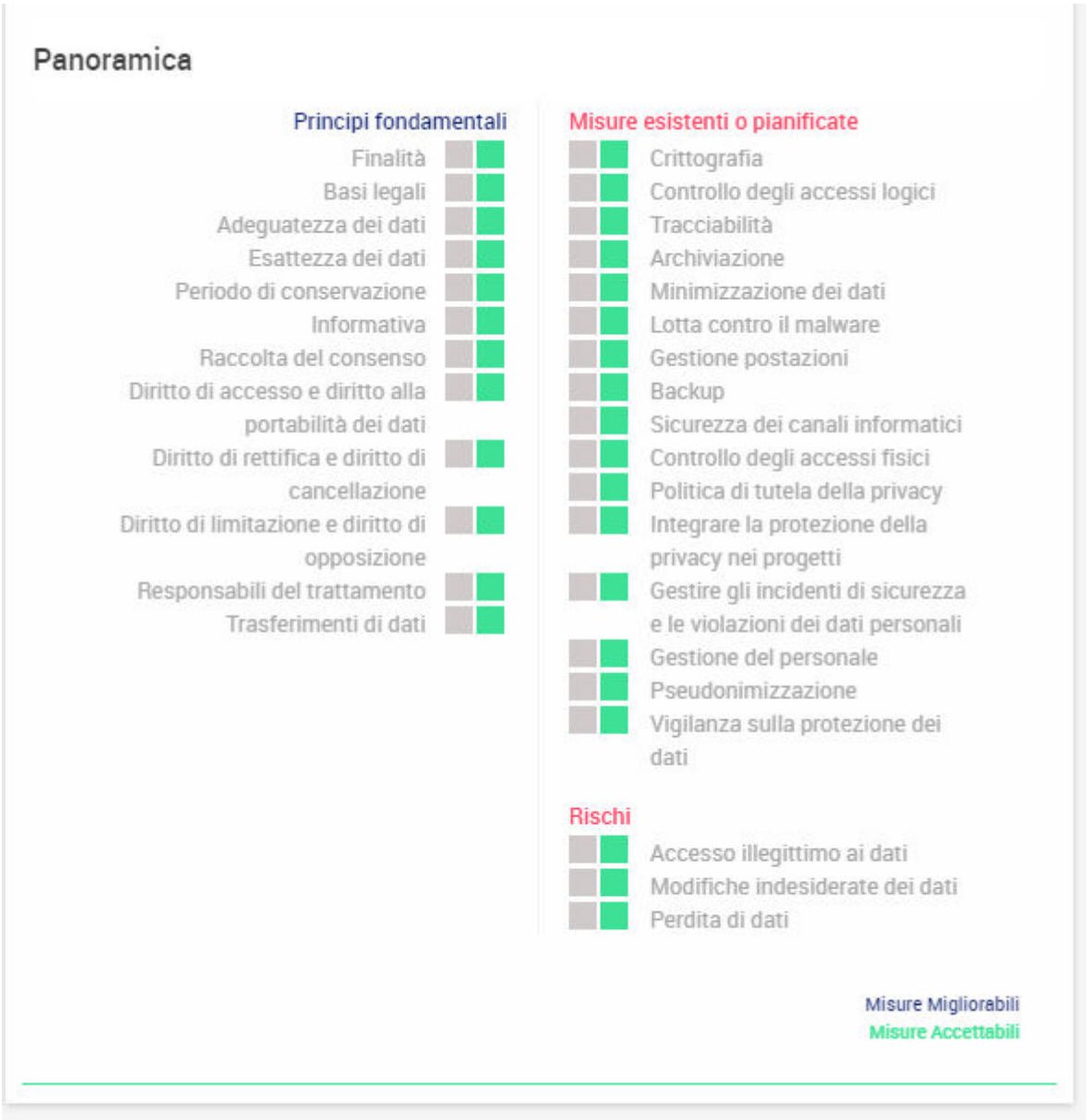
## Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

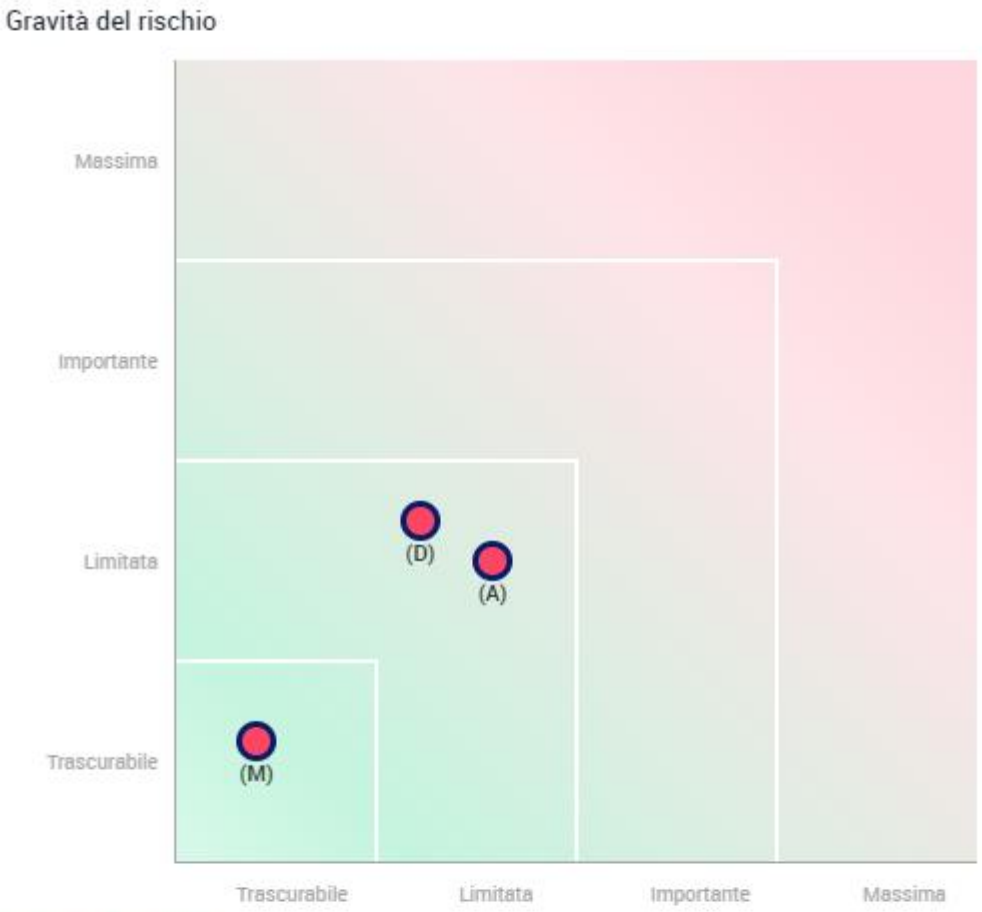
Limitata, Date le misure di minimizzazione, di pseudonimizzazione, di crittografia, backup, controllo degli accessi logici, di sicurezza dei canali informatici, e data la natura retrospettiva degli studi che prende dati comunque archiviati in altre forme come la cartella clinica informatizzata, il rischio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

**Valutazione : Accettabile**

# Rischi

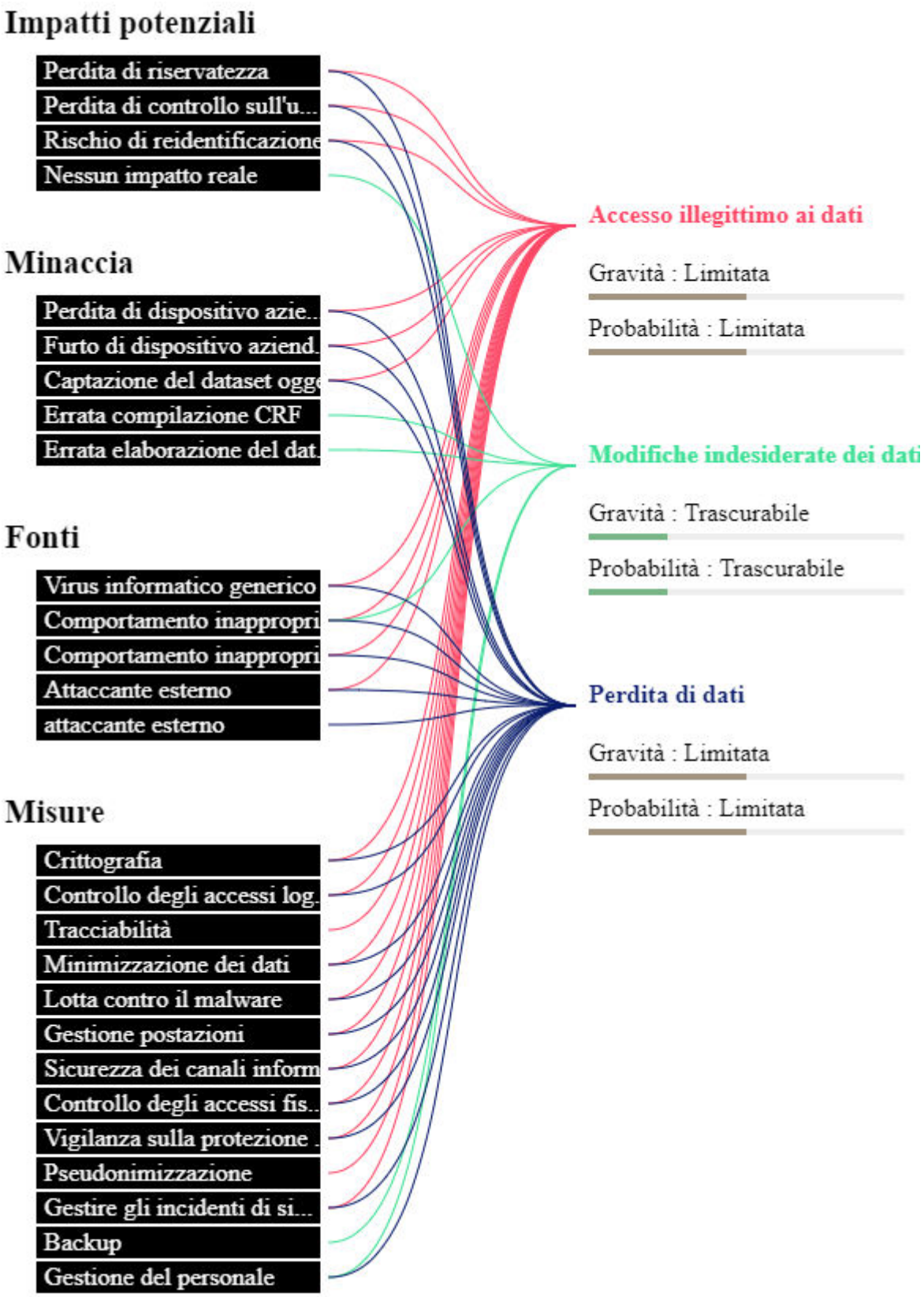
## Panoramica dei rischi






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

05/02/24


Impatti potenziali
Perdita di riservatezza
Perdita di controllo sull'u...
Rischio di reidentificazione
Nessun impatto reale
Minaccia
Perdita di dispositivo azie...
Furto di dispositivo aziend...
Captazione del dataset ogg...
Errata compilazione CRF
Errata elaborazione del dat...
Fonti
Virus informatico generico
Comportamento inappropri...
Comportamento inappropri...
Attaccante esterno
attaccante esterno
Misure
Crittografia
Controllo degli accessi log...
Tracciabilità
Minimizzazione dei dati
Lotta contro il malware
Gestione postazioni
Sicurezza dei canali inform...
Controllo degli accessi fis...
Vigilanza sulla protezione ...
Pseudonimizzazione
Gestire gli incidenti di si...
Backup
Gestione del personale
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Limitata