Valutazione d'impatto trasversale sul trattamento dei dati personali studio osservazionale multicentrico - Apache - promosso dalla Fondazione Policlinico Universitario Agostino Gemelli IRCCS di Roma.

(Versione 1.0 – 11.04.2024)

Nome del DPO
Cristina Canella DPO IOV

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Vista la natura retrospettiva dello studio in oggetto, condotto in seguito all'erogazione della prestazione di cura, date le misure di minimizzazione e 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 della perdita del controllo dei dati e della violazione della riservatezza residuo, risulta limitato. Pertanto il trattamento può essere implementato

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 e nel rispetto di quanto previsto dall'art. 89 GDPR come documentato nell'autodichiarazione formulata dai PI degli studi, sarà in ogni caso onere dell'Istituto cercare di ottenere successivamente il consenso dei pazienti non contattabili qualora questi si presentino presso lo IOV per ulteriori prestazioni sanitarie o follow up. Sul punto vedere anche specifico documento redatto dal Titolare in riferimento alla non applicabilità del consenso.

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 APACHE2 promosso dalla Fondazione Policlinico Universitario Agostino Gemelli IRCCS di Roma.

Obiettivo primario dello studio è convalidare il ruolo
predittivo della firma APACHE in termini di PFS in pazienti
trattati con diversi tipi di terapie.

Per il presente studio lo IOV-IRCCS intende arruolare almeno 30 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?

I dati trattati nel contesto della ricerca scientifica sono quelli stabiliti dal protocollo di studi e in particolare:
- dati anagrafici e di contatto;
- dati di natura particolare ex art. 9 GDPR (dati sulla salute, dati genetici);

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

Il personale sanitario impegnato nella ricerca clinica estrae manualmente i dati dalla cartella clinica del paziente e in particolare vengono riportati nella CRF elettronica e in particolare i dati che includono caratteristiche del tumore, dei trattamenti ai quali è stato sottoposto, dei controlli che sono stati effettuati dopo l'intervento chirurgico, nonché i dati relativi ai campioni biologici di pazienti colpiti dalla mutazione oggetto dello studio.
Tali dati sono trasferiti in forma pseudonimizzata al Promotore con gli strumenti di condivisione concordati con lo stesso, e sono analizzati per il tempo strettamente necessario alla conduzione dello studio (minimo 12 mesi di osservazione) al termine del quale saranno conservati per un periodo massimo di quattro anni ed eventualmente trattati, previa anonimizzazione, per finalità di pubblicazione scientifica ivi compresa la possibilità di pubblicare i raw data in accordo con la procedura approvata dall'Istituto.
Il Promotore non è tenuto a conoscere l'identità dei pazienti, se non in fase di controllo della qualità della ricerca per tramite del monitor e comunque solo *on-site* per il tempo strettamente necessario ad effettuare tali verifiche.

Quali sono le risorse di supporto ai dati?

- CRF elettronica
- Campioni biologici
- Software di office automation in dotazione all'Istituto
- Sistema informativo aziendale
- Postazioni aziendali fisse
- Rete aziendale

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 durata prevista dallo studio è di dodici mesi e i dati saranno poi conservati per ulteriori 4 anni dalla conclusione dello studio e potranno successivamente essere trattati solo in forma anonima e aggregata per la pubblicazione dei risultati della ricerca clinica e per l'eventuale pubblicazione dei raw data in conformità con la procedura operativa adottata dall'Istituto.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono edotti tramite idonea informativa pubblicata sul sito web d'istituto ad uopo compilata per i trattamenti riguardanti la ricerca scientifica.
I pazienti che dovessero eventualmente presentarsi in occasione di *follow up* o altre prestazioni di cura riceveranno l'informativa a mano e avranno la possibilità di esprimere il proprio consenso al trattamento dei dati personali.

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 come documentato nell'autodichiarazione formulata dai PI degli studi, sarà in ogni caso onere dell'Istituto cercare di ottenere successivamente il consenso dei pazienti non contattabili qualora questi si presentino presso lo IOV per ulteriori prestazioni sanitarie o *follow up.*
Sul punto vedere anche specifico documento redatto dal Titolare in riferimento alla non applicabilità del 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

Anonimizzazione

I dati vengono sottoposti ad anonimizzazione e aggregazione prima della pubblicazione dei risultati della ricerca ed eventualmente dei relativi *raw data* in conformità a quanto descritto dalla relativa procedura aziendale.

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

Archiviazione

I dati della ricerca sono caricati su foglio excel in forma pseudonimizzata, archiviati in zip, protetti da password forte che viene spedita separatamente.

Valutazione : Accettabile

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. I dati raccolti saranno trattati esclusivamente per le finalità dello Studio. 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

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

Sicurezza dell'hardware

Tutti i dispositivi in dotazione al personale dell'Istituto sono equipaggiati con antivirus costantemente aggiornato. Ogni dispositivo in custodia al personale di ricerca può essere utilizzato soltanto da personale formato ad uopo.

Valutazione : Accettabile

Politica di tutela della privacy

L'istituto ha adottato un regolamento concernente la protezione dei dati personali che descrive in maniera puntuale le modalità di gestione dei dati personali e i ruoli organizzativi.

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.
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

Gestione dei terzi che accedono ai dati

Soltanto il personale impegnato nello specifico *trial* può accedere ai dati trattati per la sperimentazione.
Il Promotore non può accedere ai dati in chiaro, soltanto il monitor da questi nominato è autorizzato a vedere tali dati in occasione di verifiche mirate sulla qualità della ricerca in linea con le "Good clinical practices" di cui al DM 15 luglio 1997, e soltanto *on-site* per il tempo strettamente necessario per le verifiche e in ogni caso con divieto di esportare i dati a cui viene dato accesso.

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

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

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?

Sottrazione delle credenziali di acceso, Attacco al sistema informatico aziendale, Attacco ali sistema informatico del promotore, Intercettazione delle comunicazioni

Quali sono le fonti di rischio?

Comportamento improprio personale interno, Comportamento improprio personale del promotore, Attaccante esterno

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Anonimizzazione, Controllo degli accessi logici, Archiviazione, Minimizzazione dei dati, Lotta contro il *malware*, Gestione postazioni, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione dei terzi che accedono ai dati, Gestione del personale, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati

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

Importante, Nonostante la natura retrospettiva degli studi che sono condotti in seguito all'erogazione delle prestazioni di cura, data le misure di minimizzazione, di pseudonimizzazione la gravità del rischio di perdita del controllo dei dati e della riservatezza residuo risulta comunque elevato in quanto l'eventuale accesso ai dati dei pazienti in chiaro, comprometterebbe la loro riservatezza e determinerebbe la mancanza di controllo sull'utilizzo dei degli impatti tanto materiali quanto immateriali significativi vista anche la categoria particolarmente vulnerabile di interessati coinvolti nel trattamento.
Si raccomanda pertanto di porre molta attenzione al processo di pseudonimizzazione, alla vigilanza sulla protezione dei dati personali, alla sicurezza dei canali informatici e alla formazione del personale 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, backup, controllo degli accessi logici, di sicurezza dei canali informatici, cifratura, passoword forte, archiviazione, formazione del personale, gestione dei terzi che accedono ai dati, la probabilità del verificarsi del rischio di eventuale accesso illegittimo dei dati residuale rimane limitata.

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 delle CRF

Quali sono le fonti di rischio?

Comportamento improprio personale interno

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

Gestione del personale

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

Trascurabile, Il rischio per i diritti e le libertà degli interessati è trascurabile, l'impatto di una modifica indesiderata avrebbe effetti unicamente sui risultati della ricerca.

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

Trascurabile, Il personale coinvolto nella ricerca è altamente qualificato e specializzato

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

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

Intercettazione delle comunicazioni, Sottrazione delle credenziali di acceso, Attacco al sistema informatico aziendale, Attacco ali sistema informatico del promotore

Quali sono le fonti di rischio?

Attaccante esterno, Comportamento improprio personale del promotore, Comportamento improprio personale interno

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

Controllo degli accessi logici, Archiviazione, Minimizzazione dei dati, Lotta contro il malware, Gestione postazioni, Backup, 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?

Importante, Nonostante la natura retrospettiva degli studi che sono condotti in seguito all'erogazione delle prestazioni di cura, data le misure di minimizzazione, di pseudonimizzazione la gravità del rischio di perdita del controllo sull'utilizzo dei dati e della riservatezza residuo risulta comunque elevato in quanto l'eventuale perdita dei dati dei pazienti in chiaro, potrebbe compromettere la loro riservatezza con degli impatti tanto materiali quanto immateriali significativi vista anche la categoria particolarmente vulnerabile di interessati coinvolti nel trattamento.
Si raccomanda pertanto di porre molta attenzione al processo di pseudonimizzazione, alla vigilanza

sulla protezione dei dati personali, alla sicurezza dei canali informatici, alla formazione del personale e agli strumenti di backup in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale perdita dei dati.

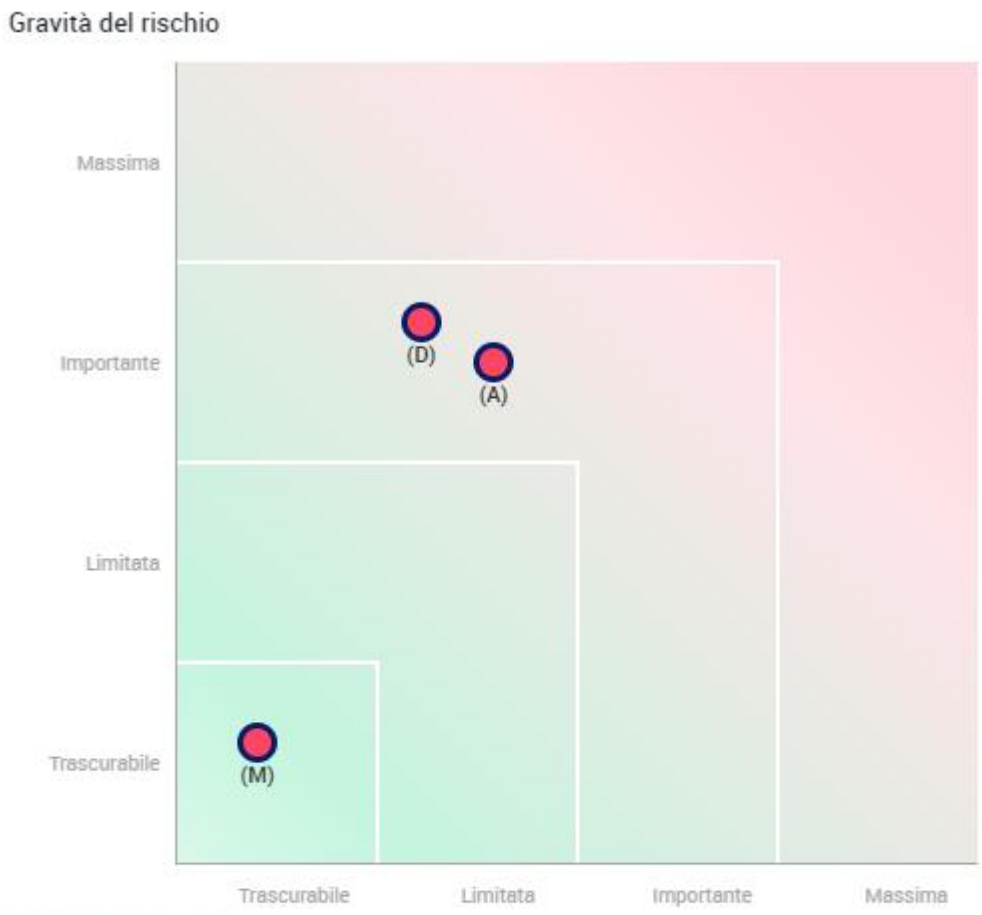
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata, Date le misure di minimizzazione, di 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 la probabilità che ciò si realizzi risulta limitato anche se si raccomanda di porre molta attenzione alla formazione e gestione del personale e backup 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.

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

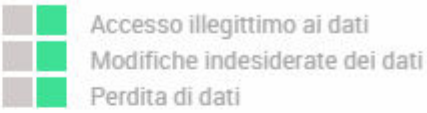
19/03/24

Panoramica

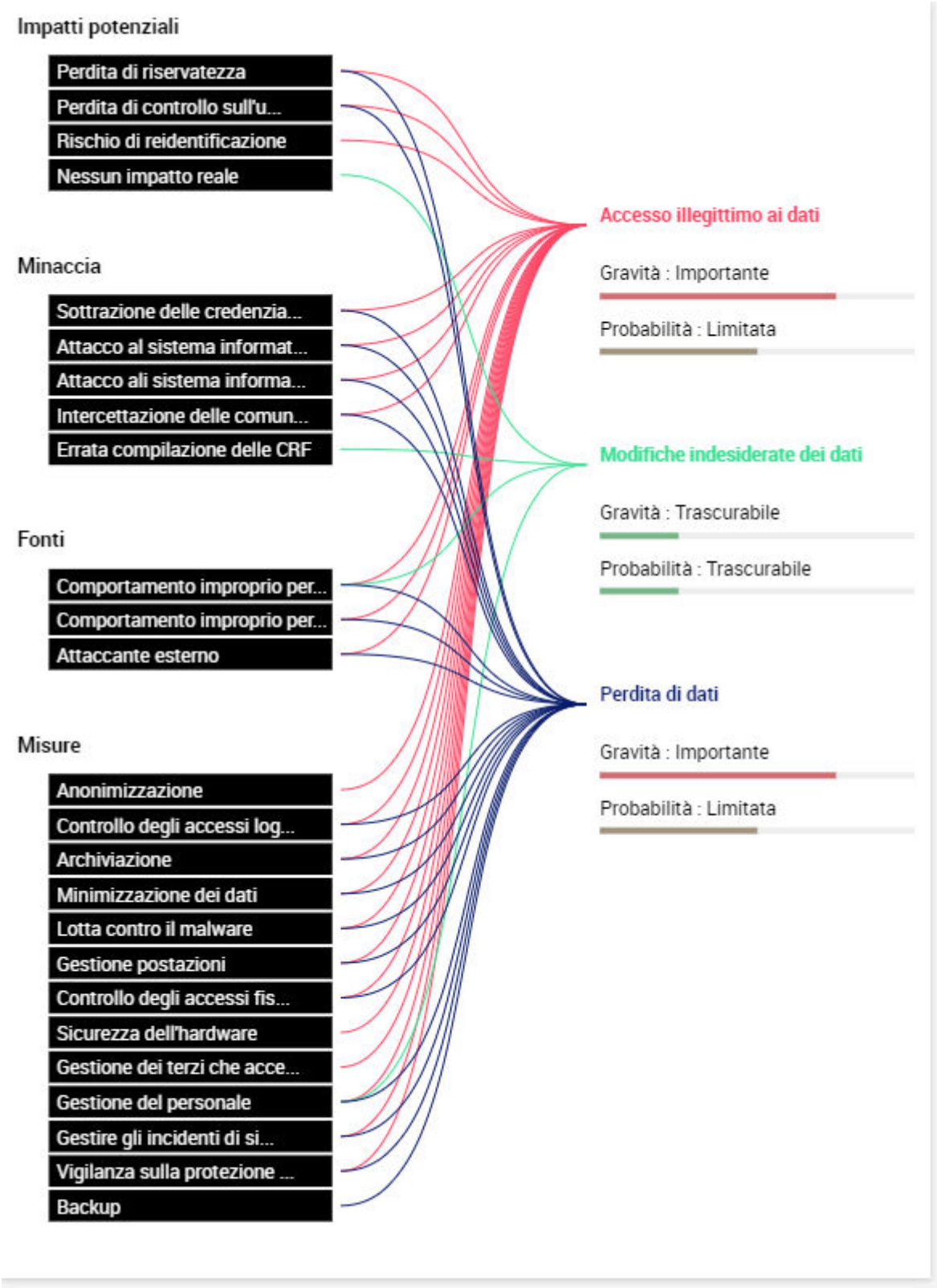
Principi fondamentali

Misure esistenti o pianificate

Rischi



Misure Migliorabili
Misure Accettabili


Impatti potenziali
Perdita di riservatezza
Perdita di controllo sull'u...
Rischio di reidentificazione
Nessun impatto reale
Minaccia
Sottrazione delle credenzia...
Attacco al sistema informat...
Attacco ali sistema informa...
Intercettazione delle comun...
Errata compilazione delle CRF
Fonti
Comportamento improprio per...
Comportamento improprio per...
Attaccante esterno
Misure
Anonimizzazione
Controllo degli accessi log...
Archiviazione
Minimizzazione dei dati
Lotta contro il malware
Gestione postazioni
Controllo degli accessi fis...
Sicurezza dell'hardware
Gestione dei terzi che acce...
Gestione del personale
Gestire gli incidenti di si...
Vigilanza sulla protezione ...
Backup
Accesso illegittimo ai dati
Gravità : Importante
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Importante
Probabilità : Limitata