Istituto Oncologico Veneto
I.R.C.C.S.

Valutazione d'impatto sullo studio EORTC-BTG-2013 PI Dott. Lombardi

Nome del DPO/RPD

Cristina Canella RPD IOV

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

a fronte delle misure tecniche organizzative predisposte, il rischio per i diritti e le libertà degli interessati può essere classificato limitato in conformità alle disposizioni dell'art.39 lett.c del Reg-2016/679 e pertanto può essere implementato.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Si ritiene il consenso non necessario in quanto il titolare è un I.R.C.C.S. che effettua gli studi analizzati con la presente valutazione nell'ambito dei programmi "...di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502.." provvedendo inoltre a condurre e rendere pubblica la presente valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento.

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 06.06.2017. Pertanto, l'Istituto svolge, nella disciplina dell' oncologia, attività di prevalente ricerca biomedica e sanitaria e di assistenza sanitaria di tipo clinico e traslazionale.
Pertanto, 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 riguarda specifici progetti di ricerca, ovvero studi osservazionali retrospettivi, con promotore esterno a 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, 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).

In questo contesto generale la presente valutazione d'impatto riguarda lo studio denominato EORTC 2013-BTG promosso da European Organisation for Research and Treatment of Cancer (EORTC).

Obiettivo dello studio è la creazione di un database per registrare i pazienti con tumore al cervello primitivo, inclusi quelli recentemente ridefiniti alla luce della riclassificazione dell'OMS del 2021, al fine di offrire profili aggiornati di malattie inclusi dati sull'età, la diagnosi, le rappresentazioni visive e cliniche, le cure disponibili e i loro effetti.

Dal protocollo di studio, gli obiettivi primari sono:

Creare una banca dati per registrare pazienti con tumori cerebrali primitivi, compresi quelli recentemente (ri)definiti nella classificazione della OMS del 2021
• Fornire profili di malattia aggiornati, compresi i dati sull'età alla diagnosi, sulla presentazione clinica e della diagnostica per immagini, trattamenti ed esiti attualmente disponibili.

Gli obiettivi secondari sono:
• Determinare se le categorie di malattia di nuova definizione (classificazione della OMS del 2021) determinino coorti di pazienti con un fenotipo clinico più omogeneo rispetto alla classificazione della OMS del 2016.
• Determinare se le previsioni degli esiti in base alla classificazione della OMS del 2021 sono più affidabili e cambierebbero l'assegnazione al trattamento.
• Caratterizzare il profilo di diagnostica per immagini neurologica di nuove entità patologiche alla presentazione e qualsiasi progressione nel corso della malattia.
• Generare dati di riferimento per i gruppi di controllo da parte dell'entità tumorale che facilitino il disegno delle sperimentazioni cliniche di nuova generazione per i pazienti con tumori cerebrali primitivi.
Obiettivi della ricerca traslazionale:
• Confermare le diagnosi istologiche e molecolari locali
Obiettivi esplorativi:
• Completare il profilo molecolare di ciascuna entità tumorale, compresa la metilazione e il sequenziamento del genoma, nonché le analisi di espressione genica.

Lo studio conta di una parte retrospettiva e di una parte prospettica.

Quali sono le responsabilità connesse al trattamento?

Le parti in forza del contratto di ricerca sono qualificate come autonomi titolari del trattamento.

Responsabile del trattamento per la parte di trasferimento dati tra titolari autonomi:

Medidata Solutions, Inc - Andrew Kopelman:

VP, AGC & Chief Privacy Counsel
Medidata Solutions, Inc.
350 Hudson St
New York, New York 10014-4535

Il responsabile del trattamento è coperto da certificazione Data Privacy Framework
come risulta da:
https://www.dataprivacyframework.gov/s/participant-search/participant-detail?id=a2zt0000000GnMVAA0&status=Active

Responsabile del trattamento per il database:

ESD (CHES) Address: Bundesstraße 9, A-6063 Rum, Austria, duly represented by Bernhard Holzner, CEO and Gerhard Rumpold, CEO.

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?

- dati di natura comune
- dati di natura particolare ex art. 9 GDPR (dati relativi allo stato di salute, dati derivanti da campioni biologici)

Nel dettaglio dal protocollo di studi:

- Età
- Morte
- Stato di salute generale
- Diagnosi
- Patologia
- Storia clinica di famiglia
- Ospedale o Identificativo del paziente
- Scan CT
- MRI Scan

- Informazioni sul farmaco prescritto
- Sesso

Per lo IOV si intendono arruolare complessivamente 80 pazienti.

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

I dati dei pazienti arruolati vengono seguiti dalla data di arruolamento a quella di morte e comunque non oltre un periodo di dieci anni, i dati vengono trasmessi al centro partecipante ogni sei mesi.
Il centro partecipante (lo IOV) invia i dati al Promotore a seguito di procedura di pseduonimizzazione con l'assistenza del servizio informatico, vengono trattati solo i dati richiesti dal CFR e il Promotore verifica che non vi siano dati eccedenti, in nessun caso il Promotore è tenuto a conoscere direttamente l'identità dei pazienti, ma tratta soltanto i dati ricevuti in forma codificata.
Solo il monitor può conoscere l'identità dei pazienti nel corso esclusivamente di attività di controllo dello studio e della qualità della ricerca "on site" e mai da remoto.
Alla conclusione dello studio il Promotore intende riutilizzare e trasferire i dati presenti a terzi non specificati al momento della stesura della presente valutazione d'impatto, sul punto è stato specificato che ogni nuovo trattamento di dati sarà portata a termine una nuova e diversa valutazione della compatibilità del trattamento in ossequio all'art. 89 GDPR.
I dati contenuti nella cartella clinica, sono a loro volta conservati in maniera illimitata in conformità alla vigente disciplina di settore e a quanto documentato nel massimario di scarto.

Quali sono le risorse di supporto ai dati?

Le principali risorse a supporto dei dati sono:
• Files di office automation ad uso dei singoli ricercatori, sia conservati su singole postazioni client che su aree di share aziendali;
• Aree condivise messe a disposizione dall'azienda, con condivisione tra i ricercatori coinvolti nel singolo progetto;
I dati vengono inviati al Promotore tramite esclusivamente tramite l'utilizzo di un CRF elettronico su piattaforma individuata dal Promotore stesso.
Il software impiegato per la condivisione è fornito da Medidata Solutions, su soluzione SaaS, con server negli Stati Uniti d'America.
Agli atti risulta che Medidata Solutions è certificato Data Privacy Framework pertanto il trattamento dei dati si presume conforme agli standard richiesti per tale certificazione, il fornitore ha documentato le proprie conoscenze in materia di sicurezza e di gestione dei dati sensibili che sono regolarmente aggiornate e certificate (certificati ISO/IEC/OCPD).
I dati sono previamente sottoposti a tecniche di pseudonimizzazione tramite l'impiego del software Amnesia sviluppato da OpenAire
https://amnesia.openaire.eu/index.html.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono specifici, espliciti e legittimi. In quanto la finalità di ricerca scientifica e gli obiettivi delle ricerca sono chiari ed espliciti dal protocollo di studi.

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 sono soltanto quelli strettamente necessari per lo svolgimento della ricerca, definiti in maniera puntuale dal protocollo di studi, e il Promotore che li riceve si impegna a non trattare i dati eventualmente eccedenti, i quali vengono cancellati da un soggetto autorizzato e istruito dal centro deputato al monitoraggio della qualità dei dati della ricerca.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

L'esattezza dei dati è garantita dalla natura dello studio che dipende dal protocollo di studio che necessità di un determinato set di dati preciso e aggiornato durante la fase di follow up dei pazienti che vengono seguiti per un totale di dieci anni.
Il Promotore verifica i criteri di eleggibilità dei pazienti in maniera specifica e indivuale, e dunque scarta i dati di quei pazienti che non rientrassero nei criteri di eleggibilità fissati dal protocollo di studi.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati relativi ai pazienti vengono conservati per un periodo di dieci anni dopo la conclusione dello studio, al termine del quale i dati devono essere distrutti. EORTC si impegna a cancellare i dati di studio con un preavviso di 30 di giorni al centro satellite.
I dati contenuti nella cartella clinica, sono a loro volta conservati in maniera illimitata in conformità alla vigente disciplina di settore e a quanto documentato nel massimario di scarto.

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?

Si ritiene il consenso non necessario in quanto il titolare è un I.R.C.C.S. che effettua gli studi analizzati con la presente valutazione nell'ambito dei programmi "...di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502.." provvedendo inoltre a condurre e rendere pubblica la presente valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Si veda anche lo 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.
Gli interessati possono inoltre contattare gli uffici del Promotore tramite una richiesta all'ufficio privacy dello IOV che si occuperà di trasmettere al Promotore le richieste degli interessati, fungendo da punto di contatto qualificato volto a facilitare l'esercizio del diritto alla protezione dei dati personali.

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.
Gli interessati possono inoltre contattare gli uffici del Promotore tramite una richiesta all'ufficio privacy dello IOV che si occuperà di trasmettere al Promotore le richieste degli interessati, fungendo da punto di contatto qualificato volto a facilitare l'esercizio del diritto alla protezione dei dati personali.

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.
Gli interessati possono inoltre contattare gli uffici del Promotore tramite una richiesta all'ufficio privacy dello IOV che si occuperà di trasmettere al Promotore le richieste degli interessati, fungendo da punto di contatto qualificato volto a facilitare l'esercizio del diritto all protezione dei dati personali.

Valutazione : Accettabile

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

Eortc nominerà Medidata responsabile del trattamento ex art. 28 GDPR con un atto formale.

Valutazione : Accettabile

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

Si prevede l'utilizzo della piattaforma Medidata RAV per il trasferimento dei dati in forma pseudonima, tale piattaforma è un sistema SaaS localizzato negli Stati Uniti. Tale sistema gode di certificazione Data Privacy Framework e pertanto offre garanzie sufficienti ad assicurare uno standard di trattamento adeguato in linea con le prescrizioni del GDPR.

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 singolo progetto 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.
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 antimalware aziendale in gestione ad AOPD; il servizio ICT sta attualmente valutando l'adozione di un nuovo sistema di protezione, migliorativo rispetto all'attuale.

Valutazione : Accettabile

Backup

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

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.
L'Istituto organizza con cadenza regolare corsi di aggiornamento e formazione del personale in materia di protezione dei dati personali.
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.
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 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

Nessun terzo può accedere ai dati personali in chiaro con esclusione del personale coinvolto nella ricerca in corso. Al Promotore il dato viene fornito solo il dato a seguito di pseudonimizzazione e senza fornire allo stesso la chiave di decodifica che è conservata dal team di ricerca IOV.
Solo il monitor può, per finalità di verifica della qualità e della correttezza della ricerca, vedere in chiaro per un tempo limitato, e soltanto "on site" e mai da remoto i dati personali dei soggetti coinvolti nel progetto di ricerca.

Valutazione : Accettabile

Restrizione d'accesso ai dati

Soltanto il P.I. e il personale da lui debitamente formato e autorizzato, possono accedere ai dati raccolti e analizzati nell'ambito del progetto di ricerca.

Valutazione : Accettabile

Anonimizzazione

Allo stato attuale l'Istituto ha adottato il software open source AMNESIA sviluppato da OpenAire, per cui ha redatto un apposito manuale.
Il servizio informatico valuta in maniera continua l'adozione di nuovi strumenti anche con licenza a pagamento.
I sistemi informativi d'Istituto sono a disposizione del personale di ricerca per il supporto all'utilizzo di questo software.

Valutazione : Accettabile

Pseudonimizzazione

Per quei dati che non possono essere anonimizzati perché altrimenti sarebbero inutilizzabili per la ricerca, l'istituto adotta per impostazione predefinita tecniche di pseudonimizzazione volte a impedire che il Promotore possa conoscere l'identità personale dei pazienti.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

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

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

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

Rischi

Accesso illegittimo ai dati

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

Perdita di riservatezza, uso inappropriato dei dati, Perdita del controllo sull'utilizzo dei dati

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?

Controllo degli accessi logici, Minimizzazione dei dati, Lotta contro il malware, Backup, Controllo degli accessi fisici, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione dei terzi che accedono ai dati, Integrare la protezione della privacy nei progetti, Pseudonimizzazione, Anonimizzazione, Sicurezza dei canali informatici

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?

errata compilazione dei crf

Quali sono le fonti di rischio?

errore umano

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?

Limitata, 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 del controllo sull'utilizzo dei dati, Perdita di riservatezza, uso inappropriato dei dati

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

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

Quali sono le fonti di rischio?

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

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

Controllo degli accessi logici, Minimizzazione dei dati, Lotta contro il malware, Backup, Controllo degli accessi fisici, Politica di tutela della privacy, Integrare la protezione della privacy nei progetti, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Pseudonimizzazione, Gestione postazioni

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

Importante, 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

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

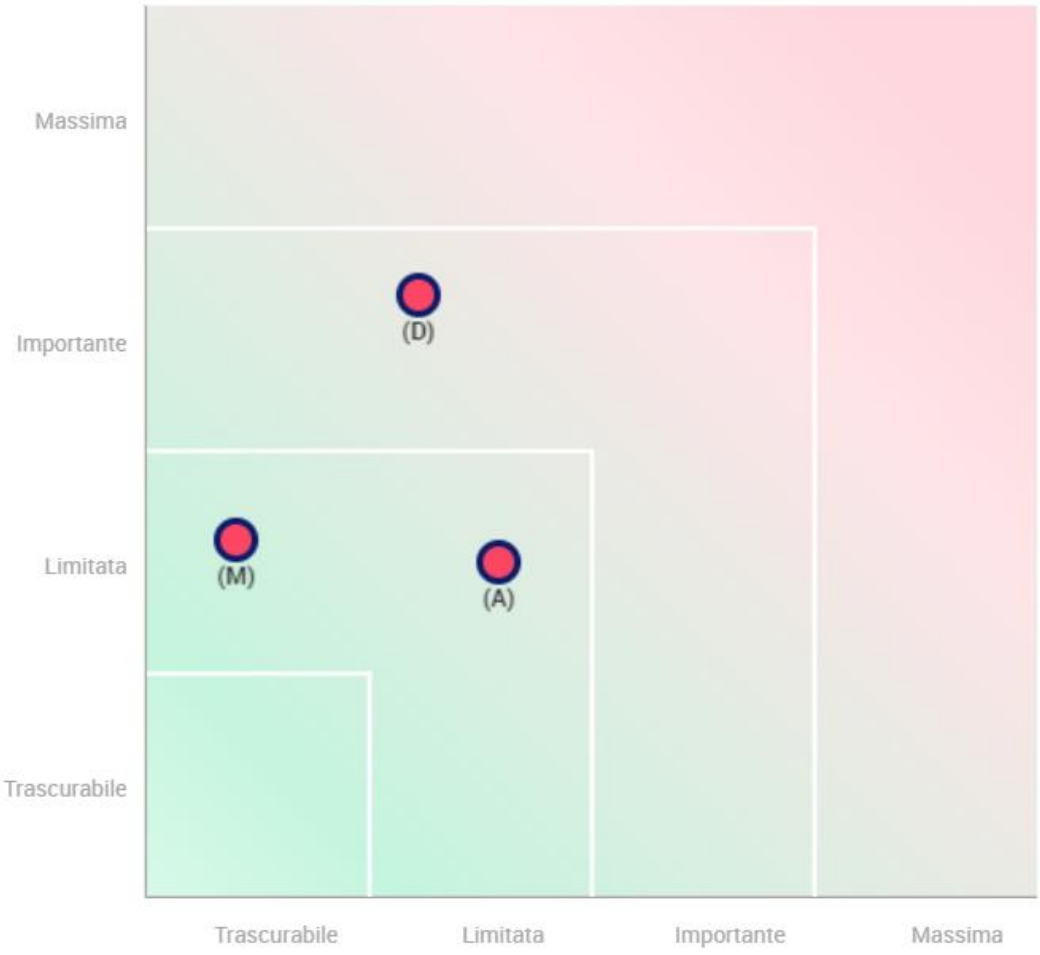
- Controllo degli accessi logici
- Minimizzazione dei dati
- Lotta contro il malware
- Backup
- Controllo degli accessi fisici
- Politica di tutela della privacy
- Integrare la protezione della privacy nei progetti
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Gestione del personale
- Gestione dei terzi che accedono ai dati
- Restrizione d'accesso ai dati
- Anonimizzazione
- Pseudonimizzazione
- Sicurezza dei documenti cartacei
- Gestione postazioni
- Sicurezza dei canali informatici

Rischi

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

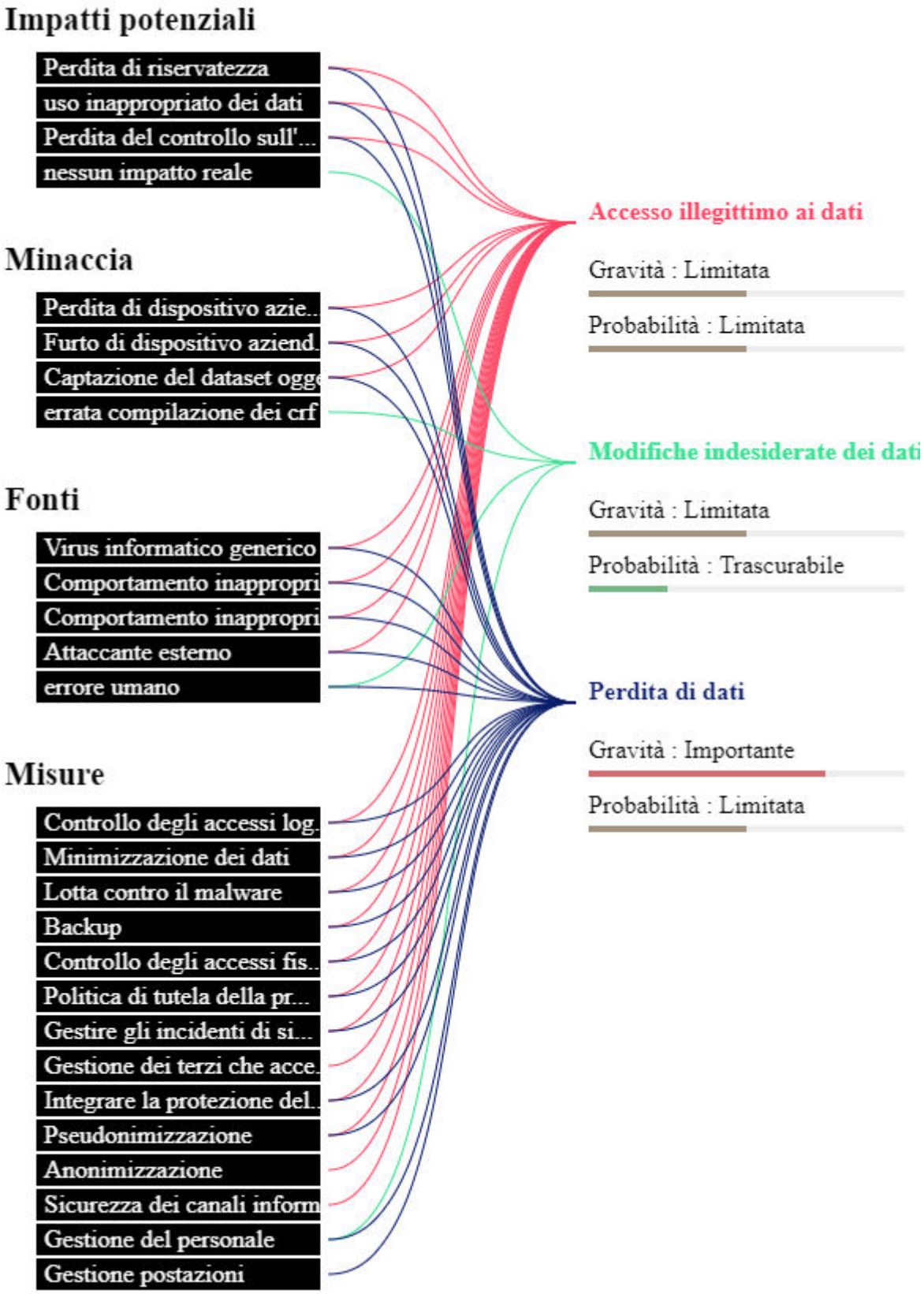
Misure Migliorabili
Misure Accettabili

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 riservatezza
uso inappropriato dei dati
Perdita del controllo sull'...
nessun impatto reale
Minaccia
Perdita di dispositivo azie..
Furto di dispositivo aziend..
Captazione del dataset ogg
errata compilazione dei crf
Fonti
Virus informatico generico
Comportamento inappropri
Comportamento inappropri
Attaccante esterno
errore umano
Misure
Controllo degli accessi log..
Minimizzazione dei dati
Lotta contro il malware
Backup
Controllo degli accessi fis..
Politica di tutela della pr...
Gestire gli incidenti di si...
Gestione dei terzi che acce..
Integrare la protezione del..
Pseudonimizzazione
Anonimizzazione
Sicurezza dei canali inform
Gestione del personale
Gestione postazioni
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Limitata
Probabilità : Trascurabile
Perdita di dati
Gravità : Importante
Probabilità : Limitata