Valutazione d’impatto sul trattamento dei dati personali studio osservazionale multicentrico -

IRFMN-OVA-8338 promosso dall''Istituto di Ricerche Farmacologiche Mario Negri - IRCCS

(Versione 1.0 – 18.03.2024)

Nome del DPO/RPD

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 dal PI dello studio Dott.ssa Tasca, 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.

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 Osservazionale Multicentrico IRFMN-OVA-8338 promosso dall''Istituto di Ricerche Farmacologiche Mario Negri - IRCCS di Milano che ha come obiettivi:

• Creare un registro retrospettivo/prospettico italiano al fine di raccogliere retrospettivamente e prospetticamente dati epidemiologici, patologici e clinici su tumori ginecologici rari utilizzando una modalità condivisa per standardizzare questa raccolta tra le diverse banche dati nazionali esistenti; • Descrivere le principali modalità di diagnosi e trattamento di questi tumori nei centri di riferimento europei;
• Diffondere le conoscenze sui tumori rari;
• Promuovere la collaborazione e il confronto tra i centri coinvolti nel trattamento di questi tumori.

Verranno raccolti i dati clinici, patologici, chirurgici e di trattamento farmacologico e/o radioterapico di pazienti affette da queste patologie che sono in cura presso i centri coinvolti oppure lo sono state in passato. Per la parte prospettica si prevede di seguire le pazienti per la raccolta dati per almeno 20 anni dalla diagnosi. Lo studio coinvolgerà circa 20 strutture ospedaliere in Italia afferenti al gruppo collaborativo di Oncologia Ginecologica MaNGO. I dati raccolti dai centri italiani saranno messi a disposizione per effettuare delle analisi condivise con altre nazioni europee afferenti al gruppo di ricerca internazionale denominato ENGOT (European Network for Gynaecological Oncological Trial groups) con cui è stata condivisa la stessa scheda di raccolta dati.

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 (anagrafici e di contatto)
- dati sanitari (dati sulla salute, dati genetici)

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

Le procedure di raccolta dati avverranno tramite un database elettronico (eCRF). Il personale IOV effettua l'estrazione dei dati necessari per la sperimentazione clinica a partire dalle carte cliniche e li inserisce nelle eCRF.
Le eCRF saranno specificamente progettate per la raccolta dei dati clinici dettagliati nel protocollo di studio. Per la raccolta dei dati verrà utilizzata l'applicazione web RedCap® (Research Electronic Data Capture).
La struttura eCRF è implementata in RedCap dall'Istituto Mario Negri di Milano con la collaborazione dei medici del gruppo MITO e MaNGO ed è stata rivista dal comitato scientifico ENGOT.
La struttura di RedCap sarà condivisa con gli altri gruppi ENGOT che partecipano a questa iniziativa con l'obiettivo di garantire un modo uniforme di raccolta dei dati e di facilitare l'esecuzione dell'analisi utilizzando i dati raccolti nei diversi paesi.
Le pazienti idonee verranno registrate nel database e a ciascun paziente verrà assegnato un numero di studio. Per le pazienti incluse, i dati raccolti prenderanno in considerazione l'anamnesi clinica, patologica, i dettagli chirurgici e terapeutici della prima diagnosi e delle recidive, l'esame istologico, il follow-up, le gravidanze successive, gli eventi di recidiva e morte. I documenti fonte della raccolta dati includeranno cartelle cliniche, radiografie e ambulatoriali.
I dati di identificazione personale saranno accessibili solo al personale del sito e all'amministratore delle eCRF e non saranno inclusi in alcun rapporto o analisi relativa allo studio.
I dati personali trattati nell'ambito dello studio clinico saranno conservati **non oltre i quindici anni dalla conclusione dello studio.**

Quali sono le risorse di supporto ai dati?

- Oncosys
- Galileo
- Redcap
- Amnesia

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?

Il periodo di conservazione indicato nella documentazione di studio è di 20 anni (durata dello studio) e 15 anni a seguito della sua conclusione.

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.

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 dal PI dello studio Dott.ssa Tasca, 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*.

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.
Gestione dei privilegi di accesso (Profilazione) secondo principio "minima autorizzazione richiesta".
L'accesso viene garantito dal dirigente incaricato per la gestione di Redcap previa richiesta motivata di accesso.

Valutazione : Accettabile

Tracciabilità

RedCap è dotato di un sistema di log interno che tiene traccia di tutti gli accessi effettuati dagli utenti.

Valutazione : Accettabile

Archiviazione

L'archiviazione dehe sono conservati su storage S3 crittografato sulla piattaforma Amazon AWS, Cluster di Milano.

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

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 ha adottato un regolamento per 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. 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

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

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.
Inoltre RedCap prevede un sistema di backup periodico automatizzato.

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

Rischi

Accesso illegittimo ai dati

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

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

Quali sono le principali minacce che potrebbero concretizzare il rischio?

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

Quali sono le fonti di rischio?

Attacchi al sistema informativo aziendale, Perdita di dispositivo aziendale, Comportamento improprio personale

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Gestione postazioni, Controllo degli accessi fisici, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Pseudonimizzazione

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?

nessuno

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

Errata compilazione eCrf, Errata elaborazione dei dati

Quali sono le fonti di rischio?

Comportamento improprio personale

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

Tracciabilità, Gestione del personale, Backup

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

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

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

Trascurabile, Evento molto improbabile vista l'alta specializzazione e motivazione del personale di ricerca.

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?

Sottrazione delle credenziali di accesso, Perdita delle credenziali di accesso, Utilizzo improprio dei dispositivi aziendali, Danni alle infrastrutture it

Quali sono le fonti di rischio?

Attacchi al sistema informativo aziendale, Comportamento improprio personale, Perdita di dispositivo aziendale, Incidenti o sinistri nei luoghi in cui sono localizzate le infrastrutture IT

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Minimizzazione dei dati, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Pseudonimizzazione, Backup, Controllo degli accessi fisici, Sicurezza dell'hardware

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

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

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

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

Valutazione : Accettabile

Rischi

Panoramica dei rischi

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

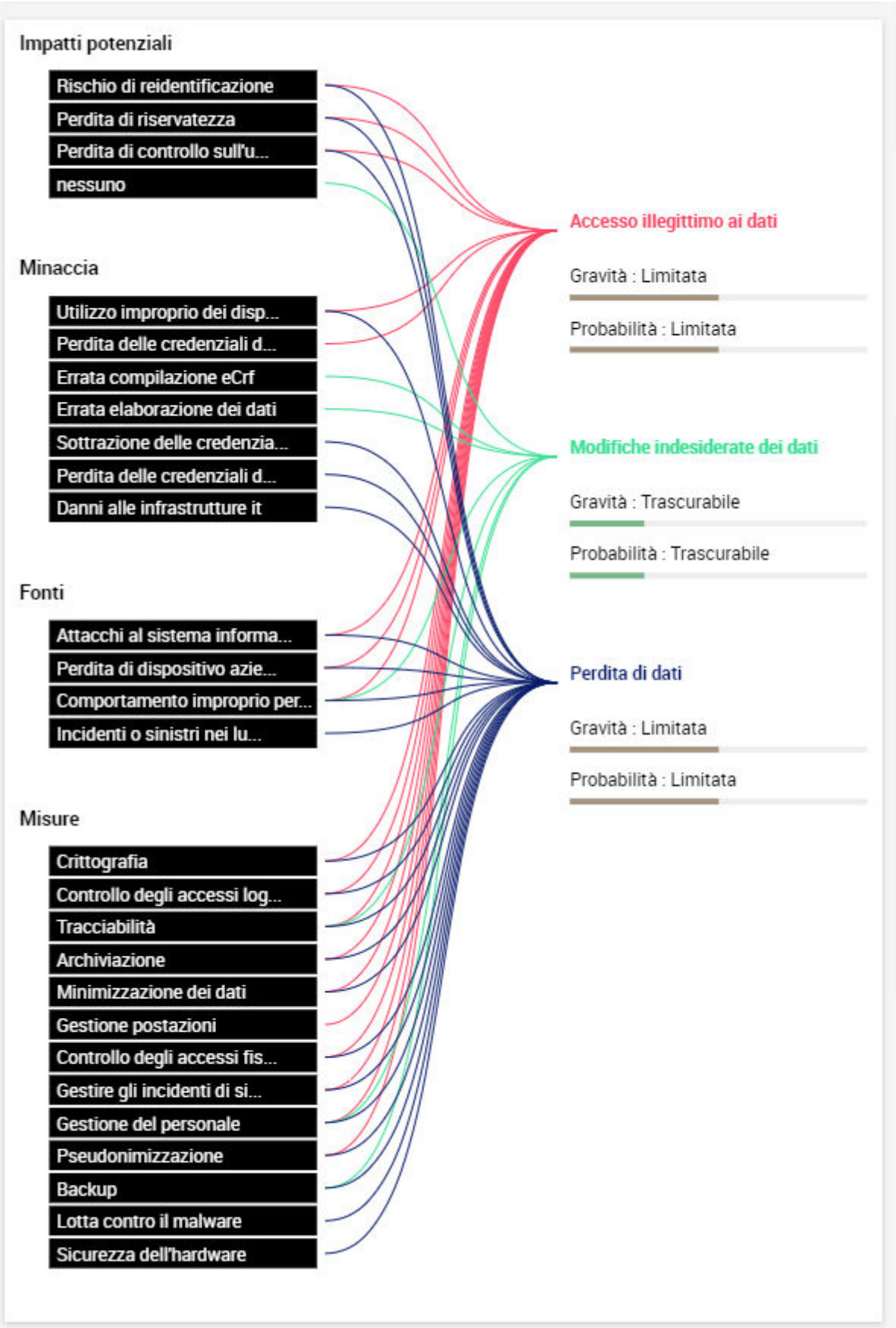
Misure esistenti o pianificate

- Crittografia
- Controllo degli accessi logici
- Tracciabilità
- Archiviazione
- Minimizzazione dei dati
- Lotta contro il malware
- Gestione postazioni
- 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
- Vigilanza sulla protezione dei dati
- Pseudonimizzazione
- Backup
- Sicurezza dell'hardware

Rischi

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

Misure Migliorabili
Misure Accettabili


Impatti potenziali
Rischio di reidentificazione
Perdita di riservatezza
Perdita di controllo sull'u...
nessuno
Minaccia
Utilizzo improprio dei disp...
Perdita delle credenziali d...
Errata compilazione eCrf
Errata elaborazione dei dati
Sottrazione delle credenzia...
Perdita delle credenziali d...
Danni alle infrastrutture it
Fonti
Attacchi al sistema informa...
Perdita di dispositivo azie...
Comportamento improprio per...
Incidenti o sinistri nei lu...
Misure
Crittografia
Controllo degli accessi log...
Tracciabilità
Archiviazione
Minimizzazione dei dati
Gestione postazioni
Controllo degli accessi fis...
Gestire gli incidenti di si...
Gestione del personale
Pseudonimizzazione
Backup
Lotta contro il malware
Sicurezza dell'hardware
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Limitata
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Limitata