



**Valutazione d’impatto sul trattamento dei dati
personali studio osservazionale multicentrico -
NIS00990 - LA-HN Italia**

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

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 NIS00990_LA-HN Italia_Ghio che ha come obiettivo primario descrivere la pratica italiana nel mondo reale per quanto riguarda le caratteristiche epidemiologiche della popolazione affetta da LA-HNSCC, le sedi di malattia, i fattori di rischio, le strategie diagnostiche e terapeutiche nel LAHNSCC, l'eventuale presenza di un team multidisciplinare.

Tra gli obiettivi ritroviamo, inoltre, l'analisi dell'impatto economico della gestione delle differenti strategie terapeutiche, tuttavia essendo uno studio osservazionale non rientra nel regolamento UE 2014/534 sulle sperimentazioni cliniche.

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 (nome, età, genere)
- dati sanitari (diagnosi, status vitale, abitudini alimentari, dipendenza da fumo, alcolismo, terapia, radioterapia, biopsia)
- dati sanitari super sensibili (positività/negatività papilloma virus, dipendenza da sostanze

stupefacenti)

- dati biometrici (superficie del corpo, peso, 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.

Popolazione di studio:

I pazienti, con età maggiore di 18 anni, devono:

- Avere avuto una diagnosi istologica o citologica di carcinoma delle labbra/cavo orale, orofaringe, ipofaringe e laringe localmente avanzato (Stadio, III, IVA, IVB, TNM VIII edizione, per pazienti HPV positivi dell'orofaringe saranno arruolati dallo stadio cT1 cN1)
- Essere stati visitati in modo consecutivo da Gennaio 2017 a Gennaio 2021.
- Avere un follow-up minimo di 15 mesi dalla fine del trattamento.
- Avere una malattia valutabile secondo criteri RECIST versione 1.1 (lesioni tumorali misurabili e non misurabili), misurata attraverso TC o RMN.
- Aver firmato il modulo di consenso informato e il modulo di privacy (se applicabile)

Tra i criteri di esclusione ritroviamo: ➤ Malattia metastatica (stadio IVC). ➤ Neoplasie del rinofaringe, cavità nasale, seni paranasali, ghiandole salivari, tiroide, carcinoma primitivo sconosciuto del distretto testa collo e carcinoma squamoso delle labbra. ➤ Avere ricevuto qualsiasi linea di trattamento a base di inibitori dei checkpoint immunitari.

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

Il personale dello IOV estrae i dati dalla cartella clinica e li condivide con il Promotore dopo averli pseudonimizzati con l'ausilio del software Amnesia. Sarà la CRO che effettuerà la raccolta dei dati pseudonimizzati dai Centri attraverso la Piattaforma denominata ACTIDE, dove i dati pseudonimizzati saranno archiviati ai fini delle verifiche di data entry, elaborazione di quesiti, reporting e analisi statistiche.

I dati trattati saranno conservati per il tempo necessario allo svolgimento della ricerca clinica al termine del quale saranno conservati per non più di cinque anni e infine distrutti.

Quali sono le risorse di supporto ai dati?

- Oncosys
- Galileo
- ACTIDE
- 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 i), in combinato disposto con l'art. 89 GDPR 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.

Non è previsto il trattamento di dati relativi alla vita sessuale o all'orientamento sessuale, nonché all'origine razziale ed etnica nel rispetto del principio di minimizzazione dei dati. I dati raccolti saranno trattati esclusivamente per le finalità dello Studio oltre che per adempiere a eventuali obblighi di farmacovigilanza previsti dalla normativa applicabile (D.M. 30.04.2015).

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 trattati per il tempo necessario alla ricerca, verranno poi conservati per finalità di verifica della qualità del trial per un periodo non superiore a 5 anni al termine del quale verranno cancellati.

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. Sul punto il PI dello studio ha compilato e sottoscritto un modulo, in uso presso l'istituto, per attestare le motivazioni che rendono impossibile l'acquisizione del consenso degli interessati.

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 software utilizzato per la condivisione dei dati è protetto da un accesso sicuro con password e i dati al suo interno sono crittografati secondo standard PGP.

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

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

I software clinici in un uso presso lo IOV per la gestione delle cartelle cliniche, e il software di condivisione messo a disposizione dal Promotore sono dotati di sistema di log volto a tracciare gli accessi ai documenti clinici.

Valutazione : Accettabile

Archiviazione

I CFR dei pazienti verranno generati e gestiti tramite gli applicativi di software 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

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 periodica le procedure e le documentazioni prodotte in ossequio al Regolamento (UE) 679/2016.

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, 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, Sottrazione delle credenziali di accesso

Quali sono le fonti di rischio?

Attacchi al sistema informativo aziendale, Perdita di dispositivo aziendale

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Pseudonimizzazione, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Integrare la protezione della privacy nei progetti

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 delle CRF, Errata elaborazione dei dati

Quali sono le fonti di rischio?

Comportamento improprio personale interno

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

Tracciabilità, Backup, Gestione del personale

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 agli applicativi, Utilizzo improprio dei dispositivi aziendali

Quali sono le fonti di rischio?

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

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

Crittografia, Controllo degli accessi logici, Tracciabilità, Lotta contro il malware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Controllo degli accessi fisici, Gestione postazioni

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

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

privacy e di minimizzazione in modo da ridurre ulteriormente il rischio ma anche gli effetti lesivi di un eventuale perdita di dati.

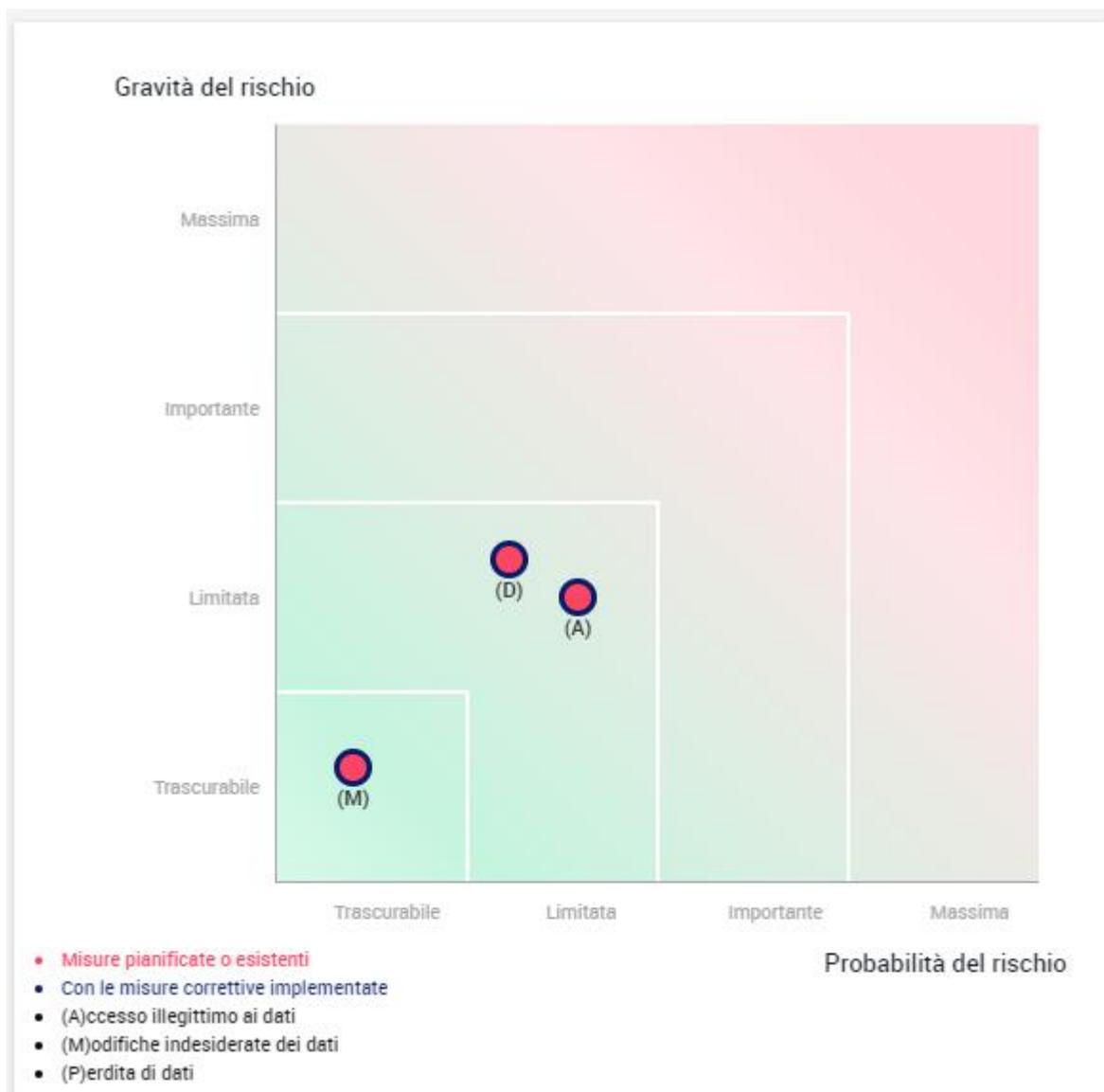
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

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

Valutazione : Accettabile

Rischi

Panoramica dei rischi



Panoramica

Principi fondamentali

Finalità	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Basi legali	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Adeguatezza dei dati	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Esattezza dei dati	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Periodo di conservazione	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Informativa	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Raccolta del consenso	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Diritto di accesso e diritto alla portabilità dei dati	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Diritto di rettifica e diritto di cancellazione	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Diritto di limitazione e diritto di opposizione	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Responsabili del trattamento	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Trasferimenti di dati	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Misure esistenti o pianificate

<input type="checkbox"/>	<input checked="" type="checkbox"/>	Crittografia
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pseudonimizzazione
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Controllo degli accessi logici
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Tracciabilità
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Archiviazione
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Minimizzazione dei dati
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lotta contro il malware
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gestione postazioni
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backup
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Politica di tutela della privacy
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Integrare la protezione della privacy nei progetti
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Gestione del personale
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Vigilanza sulla protezione dei dati
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Controllo degli accessi fisici
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sicurezza dell'hardware

Rischi

<input type="checkbox"/>	<input checked="" type="checkbox"/>	Accesso illegittimo ai dati
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Modifiche indesiderate dei dati
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Perdita di dati

Misure Migliorabili

Misure Accettabili

Impatti potenziali

- Rischio di reidentificazion...
- Rischio di reidentificazione
- Perdita di riservatezza
- Perdita di controllo sull'u...
- Nessuno

Minaccia

- Utilizzo improprio dei disp...
- Perdita delle credenziali d...
- Sottrazione delle credenzia...
- Errata compilazione delle CRF
- Errata elaborazione dei dati

Fonti

- Attacchi al sistema informa...
- Perdita di dispositivo azien...
- Comportamento improprio per...

Misure

- Crittografia
- Pseudonimizzazione
- Controllo degli accessi log...
- Tracciabilità
- Minimizzazione dei dati
- Lotta contro il malware
- Gestire gli incidenti di si...
- Integrare la protezione del...
- Backup
- Gestione del personale
- Politica di tutela della pr...
- Controllo degli accessi fis...
- Gestione postazioni

Accesso illegittimo ai dati

Gravità : Limitata

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Trascurabile

Probabilità : Trascurabile

Perdita di dati

Gravità : Limitata

Probabilità : Limitata

