La Psichiatria in Ospedale: Indagine sulle consulenze nel contesto del Dipartimento di Emergenza e Accettazione e della psichiatria di Liaison (IDEALI). Studio di tipo osservazionale multicentrico no-profit

Titolare del trattamento: AOU "Maggiore della Carità" di Novara e altri centri
Autore: Prof.ssa Carla Maria Gramaglia
Revisore: Prof.ssa Patrizia Zeppegno
Validatore: Dott. Fabrizio Leigheb

Panoramica del trattamento

Quale è il trattamento in considerazione?

La Psichiatria in Ospedale: Indagine sulle consulenze nel contesto del Dipartimento di Emergenza e Accettazione e della psichiatria di LIaison (IDEALI).

1. Lo scopo del progetto di ricerca è registrare le informazioni relative alle consulenze psichiatriche effettuate presso il DEA dell'AOU Maggiore della Carità, e delle Aziende Ospedaliere/Aziende Ospedaliero Universitarie incluse nell'elenco Centri partecipanti, (Si veda documento allegato *Elenco Centri Partecipanti alla ricerca*) allo scopo di mappare le caratteristiche, sociodemografiche e cliniche, dei soggetti che accedono al DEA per i quali vengano richieste valutazioni psichiatriche in regime di emergenza-urgenza, delineare gli elementi coinvolti nella valutazione ed intervento psichiatrico in Pronto Soccorso e l'esito delle consulenze.
2. Analogamente, scopo del progetto di ricerca è registrare le informazioni relative alle consulenze psichiatriche effettuate nel contesto della Psichiatria di Liaison-Consultazione, allo scopo di mappare le caratteristiche, sociodemografiche e cliniche, dei soggetti per i quali vengono richieste valutazioni psichiatriche durante la degenza presso altro reparto, delineare gli elementi coinvolti nella valutazione, l'intervento offerto e l'esito delle consulenze.
3. Infine, attraverso il database degli accessi per qualsiasi motivo al DEA, sarà possibile indagare più approfonditamente come l'accesso del paziente con problematica psichiatrica e la consulenza psichiatrica si collochino rispetto al flusso globale degli accessi al DEA.

Obiettivo primario
Registrare le informazioni relative alle consulenze psichiatriche effettuate presso il DEA o nel contesto della Psichiatria di Liaison-Consultazione al fine di:

- Individuare i fattori sociodemografici e clinici associati alla valutazione effettuata per "depressione" o "sintomatologia depressiva" come motivo della richiesta di consulenza;
- Individuare i fattori sociodemografici e clinici associati alla valutazione effettuata per ideazione/tentativo anticonservativo come motivo della richiesta di consulenza;
- Individuare i fattori sociodemografici e clinici associati alle consulenze psichiatriche ripetute.

Obiettivo secondario

- Valutare eventuali differenze di genere rispetto alle motivazioni ed esito delle consulenze;
- Valutare eventuali differenze tra fasce di età (giovani adulti – adulti – anziani) rispetto alle motivazioni ed esito delle consulenze;
- Valutare eventuali discordanze tra motivazioni della richiesta e sintomatologia riscontrata nel contesto delle consulenze.

Quali sono le responsabilità connesse al trattamento?

Legale rappresentante del Titolare del trattamento (DG)

Stefano Scarpetta

AOU Maggiore di Novara, Corso Mazzini n.18 - 28100 Novara,

0321 3733282

Soggetto designato con delega del Titolare

Patrizia Zeppegno

AOU Maggiore di Novara, Corso Mazzini n.18 - 28100 Novara,

0321 390 163

Responsabile della protezione dei dati (Data Protection Officer – c.d. RPD-DPO)

Slalom consulting srl – Ref. Alessandra Gaetano

Via Frosinone, 27 – 82037 Telese Terme (BN)

0824.277067

Responsabile del Trattamento

Università del Piemonte Orientale

Ci sono standard applicabili al trattamento?

No

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

1. Dati personali Comuni e Particolari, raccolti presso il DEA (Dipartimento di Emergenza e Accettazione), relativi alle consulenze psichiatriche effettuate ed estrapolati dall'applicativo PsNet:
    - Dati identificativi della consulenza psichiatrica,
    - motivo richiesta,
    - età,
    - sesso,
    - paese di nascita,
    - nazionalità,
    - città o comune di residenza,
    - stato civile,
    - scolarità,
    - professione,
    - persona che lo ha inviato al PS,
    - anamnesi psichiatrica: precedenti eventi di ricovero psichiatrico, attuali e/o precedenti accessi/cure presso SERD, diagnosi psichiatriche, terapia psicofarmacologica, comorbidità, stati di dipendenze, positività ad alcolemia e sostanze psicotrope, sintomatologia, terapia farmacologica.

2. Dati personali Comuni e Particolari, raccolti presso la Psichiatria Liaison, relativi alle consulenze psichiatriche, estrapolati dalla scheda dedicata alla raccolta dati per la Psichiatria di Liaison-Consultazione:

    - informazioni relative alla richiesta di consulenza psichiatrica,
    - informazioni cliniche e diagnostiche,
    - giorni trascorsi da eventuale evento chirurgico e comorbidità chirurgica,
    - tempo intercorso tra ricovero e richiesta di consulenza psichiatrica,
    - età,
    - informazioni su accessi o cure presso il servizio psichiatrico,
    - nazionalità,
    - stato civile,
    - necessità di mediatore,
    - presenza di supporto familiare/sociale,
    - persone con cui vive,
    - pregressa diagnosi psichiatrica,
    - esito consulenza psichiatrica,
    - terapia psicofarmacologica.

3. Dati personali Comuni, relativi al personale che partecipa allo studio:
    - Indirizzo email contenente nome e cognome dell'utente che accede alla piattaforma REDCap

Destinatari dei dati personali

I destinatari dei dati sono i Clinici/Ricercatori coinvolti nel progetto di ricerca e Università del Piemonte Orientale.

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

- **Raccolta**, Per le consulenze effettuate presso il DEA (dipartimento di emergenza e accettazione), i dati vengono estrapolati dall'applicativo aziendale PsNet; per le consulenze effettuate nel contesto della Liaison-Consultazione i dati sono raccolti su apposite schede cartacee.
- **Conservazione/archiviazione**, i dati sono archiviati su database implementati su piattaforma REDCap, dedicati rispettivamente alle consulenze effettuate in DEA (dipartimento di emergenza e accettazione) e a quelle effettuate nel contesto della Psichiatria di Liaison-Consultazione. I documenti cartacei (schede per la raccolta dati della Psichiatria di Liaison) sono conservati in luogo dedicato, in stanza chiusa e non accessibile se non al personale dedicato.
- **Distruzione**, Al completamento del periodo di conservazione previsto.

Quali sono le risorse di supporto ai dati?

- Supporti Cartacei: schede cartacee per i dati relativi alla Psichiatria di Liaison-Consultazione.
- Supporti Informatici: File Excel, applicativo aziendale "PSNet", Database REDCap.

Principi Fondamentali

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento rientranti nelle finalità di ricerca scientifica in ambito medico, biomedico ed epidemiologico (indagine statistica) sono specifici, espliciti e legittimi.

Quali sono le basi legali che rendono lecito il trattamento?

- art 6.1 lettera e: "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento";
- art 9 lettera j: "il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato".

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Sono raccolte solo le informazioni necessarie al raggiungimento delle finalità del trattamento, ossia al protocollo di ricerca.

I dati sono esatti e aggiornati?

Esattezza e aggiornamento dei dati raccolti sono garantiti dall'utilizzo di un sistema validato e protetto, tramite database implementati su piattaforma REDCap.

Qual è il periodo di conservazione dei dati?

25 anni

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'informativa specifica dello studio sarà pubblicata sul sito dell'AOU Maggiore della Carità di Novara e degli altri centri coinvolti. Non è possibile informare singolarmente gli interessati e ottenerne il relativo consenso a causa della sussistenza delle seguenti ragioni organizzative ed etiche:

- elevato numero stimato di interessati.

Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile ai sensi dell'art.110 del D.lgs.196/2003 e ss.mm.ii.

Come fanno gli interessati a esercitare i loro diritti?

La ricerca scientifica è esercitata ai sensi dell'art.110 del D.Lgs.196/2003 e ss.mm.ii., poiché non è raccolto il consenso dell'interessato, né è resa l'informativa ai singoli interessati.
Sono applicate le disposizioni di cui all'art.9, paragrafo 2, lettera j del Regolamento. Dal momento che lo studio è di tipo retrospettivo e prevede l'effettuazione di un'indagine statistica, ai sensi delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, si prevede di pubblicare sui siti dei centri di raccolta un'informativa che descrive le caratteristiche del trattamento e le modalità di esercizio dei diritti degli interessati.
Ad ogni modo, gli interessati potranno esercitare i loro diritti (di accesso, rettifica, cancellazione, limitazione e opposizione) dietro richiesta motivata alla Direzione Medica dei Presidi Ospedalieri, secondo quanto previsto nella procedura di gestione dell'esercizio dei diritti da parte dell'interessato.
Non è esercitabile il diritto alla portabilità in quanto i dati personali utilizzati nel progetto per finalità di ricerca scientifica sono stati raccolti per finalità di cura sulla base di un compito di interesse pubblico di cui è investito il Titolare del trattamento/AOU Maggiore della Carità di Novara. Con riguardo alle persone fisiche/interessati, si precisa che il trattamento non è basato su un processo decisionale automatizzato.

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

Gli obblighi dei responsabili del trattamento sono disciplinati da un atto giuridico di designazione, ai sensi dell'articolo 28 del GDPR.

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

Non è previsto il trasferimento dei dati al di fuori dell'Unione Europea.

Rischi

Misure esistenti o pianificate

Anonimizzazione

Come da protocollo, i codici fiscali dei soggetti verranno registrati solo nella scheda tecnica di raccolta dati [nota: file Excel] al fine di valutare possibili accessi multipli per patologia psichiatrica al servizio di urgenza-emergenza, dopodiché a ciascun soggetto reclutato verrà assegnato un codice numerico, registrato in forma anonimizzata sulla piattaforma REDCap, in modo da evitare qualsiasi riconoscimento e rischio di risalire alla persona fisica/interessato alla quale appartengono i dati. Il detto file Excel sarà accessibile esclusivamente ai ricercatori dei singoli centri, al solo fine di consentire l'identificazione di accessi multipli presso Dipartimento di Emergenza e Accettazione o nel contesto della Psichiatria di Liaison-Consultazione.

Controllo degli accessi logici

Username e password, sia per l'accesso ai PC aziendali, sia per accesso al database REDCap.

Tracciabilità

Accessi al database REDCap tracciabili dal gestore del database, File di Log.

Archiviazione

Come sopra descritto: cloud per il Database REDCap in concessione da parte di UPO; documenti cartacei (scheda di raccolta dati per Psichiatria di Liaison-Consultazione) conservati in luogo chiuso non accessibile a personale non autorizzato.

Sicurezza dei documenti cartacei

Come sopra descritto: documenti cartacei (scheda di raccolta dati per Psichiatria di Liaison-Consultazione) conservati in luogo chiuso non accessibile a personale non autorizzato.

Minimizzazione dei dati

Verranno raccolte solo le informazioni necessarie al raggiungimento delle finalità del trattamento, ossia del protocollo di ricerca; la riduzione del potenziale identificativo avverrà come sopra descritto: "i codici fiscali dei soggetti verranno registrati solo nella scheda tecnica di raccolta dati [nota: file Excel] al fine di valutare possibili accessi multipli per patologia psichiatrica al servizio di urgenza-emergenza, dopodiché a ciascun soggetto reclutato verrà assegnato un codice numerico, registrato in forma anonima sulla piattaforma REDCap, in modo da evitare qualsiasi riconoscimento". Il file Excel di cui in nota qui sopra, sarà accessibile esclusivamente ai ricercatori, esclusivamente al fine di consentire l'identificazione di accessi multipli presso Dipartimento di Emergenza e Accettazione o nel contesto della Psichiatria di Liaison-Consultazione.

Vulnerabilità

Per limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività, verranno documentate le procedure operative, software e hardware saranno inventariati e aggiornati, sarà limitato l'accesso fisico al materiale, e quello ai database implementati su piattaforma REDCap.

Lotta contro il malware

La protezione dei dati personali sarà garantita dai sistemi di sicurezza garantiti dalla piattaforma REDCap su cui sono implementati i database.

Gestione postazioni

La protezione dei dati personali sarà garantita dal fatto che l'accesso ai PC è protetto da username e password, così come quello alla piattaforma REDCap su cui sono implementati i database.

Sicurezza dei siti web

Come sopra riportato, l'accesso ai PC è protetto da username e password, così come quello alla piattaforma REDCap su cui sono implementati i database. Presente inoltre firewall aziendale per accesso a internet.

Backup

Backup giornaliero dei dati effettuato da REDcap.

Manutenzione

Manutenzione fisica dei dispositivi informatici da parte del CED Aziendale.

Contratto con il responsabile del trattamento

Sottoscrizione dell'atto giuridico di nomina del responsabile del trattamento tra AOU Maggiore della Carità di Novara/Titolare del trattamento e Università del Piemonte Orientale/Responsabile del trattamento.

Sicurezza dei canali informatici

Come sopra riportato, l'accesso ai PC è protetto da username e password, così come quello alla piattaforma REDCap su cui sono implementati i database. Presente, inoltre, firewall aziendale per accesso a internet.

Controllo degli accessi fisici

Accesso fisico ai locali (con porte chiuse a chiave) consentito solo a personale sanitario; accesso a materiali cartacei limitato ai clinici-ricercatori.

Sicurezza dell'hardware

Accesso fisico ai locali (con porte chiuse a chiave) che ospitano l'hardware utilizzato per la ricerca, consentito solo a personale sanitario (clinici-ricercatori).

Prevenzione delle fonti di rischio

Accesso fisico ai locali (con porte chiuse a chiave) in cui sono conservati hardware e materiali cartacei consentito solo a personale sanitario di clinici-ricercatori; presidio dei locali ove si svolge il trattamento dei dati personali.

Protezione contro fonti di rischio non umane

Sistemi di sicurezza e protezione nei confronti di fonti di rischio non umane dell'AOU, inclusi sistemi antincendio.

Politica di tutela della privacy

Legale rappresentante del Titolare del trattamento (DG): Stefano Scarpetta, AOU Maggiore di Novara, Corso Mazzini n.18 - 28100 Novara, 0321.3733282

Soggetto designato con delega del Titolare: Patrizia Zeppegno, AOU Maggiore di Novara, Corso Mazzini n.18 - 28100 Novara, 0321.3733268

Responsabile della protezione dei dati (Data Protection Officer – c.d. RPD-DPO): Slalom consulting srl – Ref. Alessandra Gaetano Via Frosinone, 27 – 82037 Telese Terme (BN) 0824.277067

Gestione delle politiche di tutela della privacy

Sono definite regole e responsabilità a livello aziendale in materia di sicurezza e protezione dei dati personali e a livello di ruoli e responsabilità del progetto e dei relativi servizi connessi (es. procedure operative in ambito ICT, distribuzione delle responsabilità, trasferimento dei dati dal perimetro aziendale verso l'esterno, etc.).

Gestione dei rischi

È definito un modello per l'analisi, la valutazione e il trattamento dei rischi di sicurezza e privacy, attraverso il software DPM (Data Protection Management). Effettuazione della presente valutazione d'impatto (DPIA).

Integrare la protezione della privacy nei progetti

Sono definite le istruzioni per l'esecuzione del trattamento (principi, regole da applicare nel trattamento, procedure, linee guida, manuali di organizzazione del servizio ecc..)
Sono definite le procedure/istruzioni di lavoro per la gestione degli incidenti che possano comportare violazione di dati personali (*data breach*).

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

A livello aziendale è stata implementata ed adottata una procedura per la gestione degli incidenti di sicurezza e per la gestione delle violazioni dei dati personali, con il coinvolgimento delle strutture che effettuano e governano gli specifici processi, che possono implicare anche un trattamento di dati personali. Per il trattamento in oggetto le strutture operative direttamente coinvolte in eventuali incidenti sono: la Direzione Medica di Presidio-Clinical Trial Center Aziendale; DPO, Gruppo privacy interno all'Ente, Struttura dei sistemi operativi.

Gestione del personale

Definizione delle responsabilità e dei profili autorizzativi; individuazione e designazione delle persone autorizzate a trattare i dati; rilascio di istruzioni per un trattamento sicuro e corretto; formazione al personale in ambito di protezione dei dati personali.

Gestione dei terzi che accedono ai dati

Non applicabile, in quanto non è previsto l'accesso di soggetti terzi ai dati della ricerca.

Vigilanza sulla protezione dei dati

Adozione di adeguate misure tecniche ed organizzative; coinvolgimento del DPO, conservazione file di log e di altri strumenti di tracciamento di eventuali anomalie, Audit di sistema, riunioni periodiche con il gruppo privacy interno all'AOU e con il DPO, assegnazione di obiettivi privacy all'unità operativa di riferimento, etc.

Rischi

Accesso illegittimo ai dati

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

Diffusione di dati sullo stato di salute dei soggetti.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso di personale non autorizzato alle aree di conservazione dei documenti cartacei, attacchi hacker, phishing delle credenziali di accesso ai PC e ai database su piattaforma REDCap.

Quali sono le fonti di rischio?

Fattori umani, malfunzionamento dei sistemi di tipo informatico (ICT), minacce che potrebbero causare una violazione (es: attacco informatico).

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Sicurezza dell'hardware, Sicurezza dei documenti cartacei, Sicurezza dei siti web, Gestione postazioni, Controllo degli accessi fisici, Gestione del personale.

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

Limitata: Presenza di molteplici misure di sicurezza (hardware e materiali cartacei utilizzati per la ricerca conservati in locali chiusi a chiave, ad accesso limitato al personale sanitario clinico-ricercatore. PC protetti da password; database REDCap accessibili solo con username e password) tali da mitigare i rischi ad un livello limitato.

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

Limitata: Presenza di molteplici misure di sicurezza (hardware e materiali cartacei utilizzati per la ricerca conservati in locali chiusi a chiave, ad accesso limitato al personale sanitario clinico-ricercatore. PC protetti da password; database REDCap accessibili solo con username e password, file di log) tali da mitigare i rischi ad un livello limitato.

Rischi

Modifiche indesiderate dei dati

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

Non si prevede il verificarsi di un impatto sugli interessati e in particolare sui loro diritti e libertà; un'eventuale modifica indesiderata dei dati avrebbe un impatto sullo studio osservazionale, senza conseguenze per gli interessati.

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

Accesso di personale non autorizzato alle aree di conservazione per documenti cartacei; attacchi hacker, phishing delle credenziali di accesso ai PC e ai database su piattaforma REDCap.

Quali sono le fonti di rischio?

fattori umani, malfunzionamento dei sistemi di tipo informatico (ICT), minacce che potrebbero causare una violazione (es: attacco informatico).

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

Gestione del personale, Sicurezza dei documenti cartacei, Backup, Controllo degli accessi fisici, Controllo degli accessi logici, Sicurezza dell'hardware

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

Limitata: Presenza di molteplici misure di sicurezza (hardware e materiali cartacei utilizzati per la ricerca conservati in locali chiusi a chiave, ad accesso limitato al personale sanitario clinico-ricercatore. PC protetti da password; database REDCap accessibili solo con username e password) tali da mitigare i rischi ad un livello limitato.

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

Limitata: Presenza di molteplici misure di sicurezza (hardware e materiali cartacei utilizzati per la ricerca conservati in locali chiusi a chiave, ad accesso limitato al personale sanitario clinico-ricercatore. PC protetti da password; database REDCap accessibili solo con username e password) tali da mitigare i rischi ad un livello limitato.

Rischi

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Non si prevede il verificarsi di un impatto sugli interessati e in particolare sui loro diritti e libertà; un'eventuale perdita indesiderata dei dati avrebbe un impatto sullo studio osservazionale, senza conseguenze per gli interessati.

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

Accesso di personale non autorizzato alle aree di conservazione per documenti cartacei, attacchi hacker, phishing delle credenziali di accesso ai PC e ai database su piattaforma REDCap.

Quali sono le fonti di rischio?

fattori umani, malfunzionamento dei sistemi di tipo informatico (ICT), minacce che potrebbero causare una violazione (es: attacco informatico).

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

Backup, Controllo degli accessi logici, Sicurezza dei documenti cartacei, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestione del personale, Tracciabilità

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

Limitata: Presenza di molteplici misure di sicurezza (hardware e materiali cartacei utilizzati per la ricerca conservati in locali chiusi a chiave, ad accesso limitato al personale sanitario clinico-ricercatore. PC protetti da password; database REDCap accessibili solo con username e password) tali da mitigare i rischi ad un livello limitato.

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

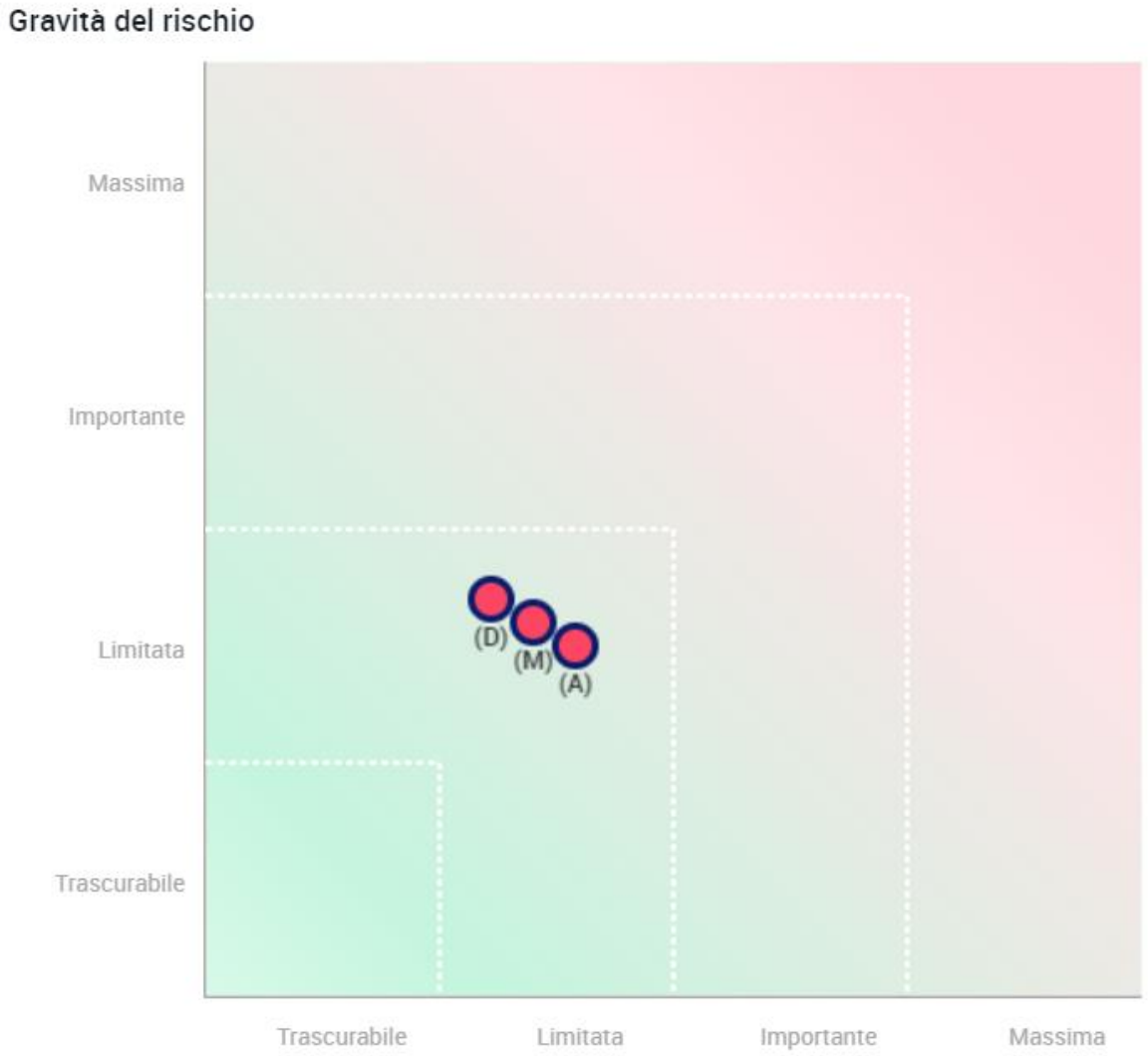
Limitata: Presenza di molteplici misure di sicurezza (hardware e materiali cartacei utilizzati per la ricerca conservati in locali chiusi a chiave, ad accesso limitato al personale sanitario clinico-ricercatore. PC protetti da password; database REDCap accessibili solo con username e password) tali da mitigare i rischi ad un livello limitato.

Azienda Ospedaliero-Universitaria
Maggiore della Carità
di Novara

SEDE LEGALE: Corso Mazzini, 18
28100 Novara - Tel. 0321.3731
www.maggioreosp.novara.it

Cod. Fiscale - Part. IVA: 01521330033

Mappatura 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

31/07/24

Panoramica dei rischi