Valutazione di impatto sulla protezione dei dati (DPIA) del paziente nello studio PERICLE RWE

Studio Real World, retrospettivo, multicentrico, di coorte, osservazionale, per valutare il profilo di sicurezza ed efficacia della Clevidipina, nella gestione dell'ipertensione peri operatoria nell'ambito delle unità di terapia intensiva italiane

Edito da: Luigi Visani (AIMED srl)

Rivisto & Approvato da: Gianluca Paternoster (ITACTAIC)

Panoramica del Trattamento

Quale è il trattamento in considerazione?

il trattamento preso in considerazione in questa DPIA si riferisce alla necessità di minimizzare il rischio di violazione dei dati personali durante la fase critica che intercorre tra l'identificazione dei pazienti idonei dalle cartelle cliniche ospedaliere da parte del medico ricercatore e la de-identificazione automatica e completa degli stessi dati che avverrà entro un tempo massimo di 60 minuti dal momento in cui, in forma pseudonimizzata sono stati inseriti nella piattaforma di anonimizzazione.
Poichè tali dati personali attengono alla salute del paziente, quali per esempio la registrazione dei valori pressori, della frequenza cardiaca, temperatura, frequenza respiratoria, sintomatologia, assunzione delle terapie in studio e di terapie concomitanti, ricadono tra le categorie particolari di dati di cui all'art 9 del Regolamento UE 679/ 2016 ("GDPR") e, pertanto, sono trattati con le particolari cautele, prescrizioni e misure di sicurezza appropriate e comunque in linea con quanto disposto dal GDPR
Come descritto in dettaglio nelle sezioni successive, il processo previsto per lo studio PERICLE garantisce che i dati siano resi anonimi il più rapidamente possibile, riducendo il rischio di esposizione o accesso non autorizzato.

Quali sono le responsabilità connesse al trattamento?

Nel contesto del trattamento dei dati nello studio PERICLE, con il caricamento e la de-identificazione automatica dei dati pazienti attraverso l'applicativo fornito da AIMED srl, le responsabilità di ciascun soggetto coinvolto sono le seguenti:

1. Titolare e Co-titolare del Trattamento *(Centro Clinico Partecipante - Promotore Studio)*

Il titolare del trattamento nella veste di centro clinico partecipante allo studio:

- Decide le finalità e i mezzi del trattamento dei dati personali, ossia l'identificazione e la raccolta dei dati dei pazienti idonei.
- È responsabile della raccolta dei dati direttamente dalle cartelle cliniche dei pazienti e del loro inserimento nell'applicativo messo a disposizione da AIMED S.r.l., società incaricata dal promotore dello studio della gestione dei dati (ITACTAICD).
- Deve garantire che i dati dei pazienti verranno raccolti e caricati nell'applicativo in forma pseudo-anonimizzati come da GDPR.
- È responsabile di implementare adeguate misure tecniche e organizzative per proteggere i dati personali fino al momento della completa de-identificazione, che avverrà entro il termine massimo di 60 minuti dal momento in cui i dati pseudo-anonimizzati del paziente sono stati caricati dal ricercatore nell'applicativo e validati.

- Deve garantire che i dati che riceve dai vari centri partecipanti siano stati precedentemente de-identificati in maniera irreversibile.
- Deve formare i vari sperimentatori sulle corrette procedure da eseguire per tale scopo e monitorare accuratamente il processo.

2. Responsabile del Trattamento *(AIMED S.r.l.)*

AIMED S.r.l., in qualità di fornitore, per il Promotore, dell'applicativo per la de-identificazione dei dati, agisce come *responsabile del trattamento*. Le sue responsabilità includono:

- Fornire e gestire l'applicativo utilizzato dai ricercatori per la raccolta e la de-identificazione dei dati dei pazienti.
- Assicurare il corretto funzionamento dell'applicativo garantendo che i dati vengano automaticamente de-identificati entro il tempo massimo previsto (60 minuti), utilizzando processi conformi alle normative e standard di sicurezza.
- Implementare misure di sicurezza, come crittografia, accesso controllato e monitoraggio continuo, per proteggere i dati durante il loro trattamento e garantire che i dati siano resi anonimi senza possibilità di re-identificazione, prima della loro esportazione e successiva analisi.
- Stipulare un contratto con il Promotore dello studio, titolare del trattamento, che stabilisca chiaramente le responsabilità e le istruzioni per il trattamento dei dati personali.

3. Eventuali altri Co-Titolari del Trattamento *(Nessuno)*

Pur essendo uno studio multicentrico, tuttavia i centri clinici partecipanti non condividono in alcun modo l'accesso e la visione di alcun dato degli altri centri.

4. Soggetti Autorizzati al Trattamento *(Personale del Centro Clinico)*

Il personale del centro clinico che accede e gestisce i dati dei pazienti (medici, infermieri, ricercatori) agisce come *soggetto autorizzato al trattamento*. Le loro responsabilità includono:

- Accesso ai dati: Accedere e inserire i dati dei pazienti nel sistema per la de-identificazione seguendo le istruzioni e le politiche del titolare del trattamento.
- Protezione dei dati: Garantire che i dati siano trattati in modo sicuro e confidenziale, limitando l'accesso ai soli soggetti autorizzati.
- Formazione: Ricevere la formazione adeguata in materia di protezione dei dati personali e conformità alle normative vigenti.

Ci sono standard applicabili al trattamento?

- Nello studio PERICLE i dati saranno completamente de-identificati prima di essere esportati fuori dal centro per essere processati ed analizzati e quindi non saranno più soggetti ai requisiti richiesti dal GDPR. Esiste tuttavia un breve periodo di tempo, prima della loro de-identificazione, che al massimo potrà essere di 60 minuti, durante il quale i dati sono ancora pseudo-anonimizzati per cui sia il Codice Privacy italiano sia il GDPR rimane applicabile. In particolare:
    - L'art. 110 del Codice Privacy modificato dal Provvedimento n. 298/2024 del Garante per la Protezione dei Dati Personali, ha chiarito le condizioni per l'utilizzo dei dati sanitari raccolti senza consenso informato.
        - *È possibile trattare i dati sanitari senza il consenso del paziente solo quando:*
            - *È impossibile o estremamente difficile ottenere il consenso (oggettive difficoltà).*
            - *Il trattamento è giustificato da finalità di ricerca scientifica o statistica in campo sanitario.*
        - *Viene richiesta una valutazione rigorosa delle misure di sicurezza e delle tecniche di pseudonimizzazione o anonimizzazione applicate ai dati.*

    - L'art.1 del GDPR Considerando 4 che recita testualmente:

        "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo.

        Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità……"

  Lo studio PERICLE si avvale della deroga al consenso, basandosi sul fatto che:

    - Trattandosi di uno studio che intende analizzare il decorso clinico nell'immediato periodo post-operatorio di pazienti che hanno subito un intervento di cardio-chirurgia maggiore, è evidente che l'acquisizione del consenso per l'utilizzo secondario dei dati è impraticabile da ottenere, sia perché diversi pazienti, nel frattempo sono deceduti, sia perché si verrebbe a creare un'inutile disagio al paziente, che dovrebbe recarsi al centro clinico solo per un atto amministrativo, ma senza averne il ben che minimo beneficio clinico.
    - La ricerca clinica è chiaramente anche nell'interesse pubblico.
    - I dati sono pseudonimizzati nel periodo critico prima dell'anonimizzazione, in linea con le disposizioni del GDPR e con le misure richieste dal Provvedimento 298/2024.
    - Sicurezza dei dati (Art. 32): Durante il periodo in cui i dati sono pseudo-anonimizzati, verranno essere implementate adeguate misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio. Questo include l'uso di crittografia, controlli sugli accessi e la gestione sicura delle chiavi per i dati pseudo-anonimizzati che saranno note solamente al personale del centro direttamente coinvolto nello studio.

- Principio di minimizzazione dei dati (Art. 5/1c): Anche se i dati sono pseudo-anonimizzati temporaneamente, saranno ridotti al minimo necessario per la finalità dello studio.

Dati, Processi e Risorse di Supporto

Quali sono i dati trattati?

Nella fase di pre-anonimizzazione vengono trattati dallo staff dello studio i dati clinici pseudonimizzati dei pazienti che sono stati identificati dai medici ricercatori rispondenti ai criteri di inclusione ed esclusione previsti dallo studio PERICLE.

Qual è il ciclo di vita del trattamento dei dati?

Di seguito una descrizione dettagliata del ciclo di vita dei dati relativi alla fase di pre-anonimizzazione, quando i dati vengono prima identificati e selezionati e poi inseriti in forma pseudonimizzata dai medici ricercatori nell'applicativo fornito da AIMED per la successiva anonimizzazione. Questo processo prevede diversi step, che vanno dalla raccolta all'analisi finale dei dati.

Fase	Descrizione
1. Raccolta dei Dati	I medici ricercatori raccolgono i dati dei pazienti dalle cartelle cliniche ospedaliere dei pazienti selezionati per lo studio, senza includere informazioni identificative dirette. Questi dati includono informazioni cliniche pertinenti, come misurazioni pressorie, trattamenti antiipertensivi, complicanze emorragiche, esiti clinici, ma senza includere informazioni direttamente identificabili come nome, cognome, e codice fiscale.
2. Pseudonimizzazione e caricamento dati	I dati vengono inseriti manualmente dai medici ricercatori nell'applicativo fornito da AIMED già pseudonimizzati. Questo processo avviene in un ambiente protetto con accesso mediante PW e riservato solo al personale autorizzato.
3. Conservazione Temporanea dei dati	I dati pseudonimizzati vengono temporaneamente conservati in locale nell'applicativo per un massimo di 60 minuti, in attesa dell'anonimizzazione completa. Durante questa fase, i dati sono protetti tramite crittografia avanzata e sono accessibili solo ai ricercatori autorizzati.
4. Anonimizzazione	Qualora il ricercatore non attivi prima il processo, entro un massimo di 60 minuti dall'inserimento, i dati che il ricercatore avrà flaggato come completi, verranno anonimizzati tramite l'applicativo. Durante questo processo, qualsiasi informazione

	che potrebbe ricondurre all'identità del paziente viene definitivamente rimossa o trasformata in modo irreversibile. L'anonimizzazione è eseguita tramite algoritmi certificati che garantiscono che i dati non possano più essere collegati all'identità dei pazienti in modo diretto o indiretto. I dati che allo scadere dei 60 minuti non saranno stati flaggati dal ricercatore come completi e che quindi non potranno essere anonimizzati, verranno automaticamente cancellati dall'applicativo. Il ricercatore dovrà quindi procedere ad un secondo inserimento manuale cercando di rispettare i tempi della procedura.
5. Esportazione dei dati anonimizzati	I dati anonimizzati vengono poi esportati e caricati in uno specifico applicativo web-based per lo studio PERICLE, il quale prima di confermare il buon esito del caricamento dei dati, provvede ad un controllo di qualità sui dati alla ricerca di eventuali dati personali e sensibili erroneamente sfuggiti alla procedura di anonimizzazione. Nel caso questo scenario si dovesse verificare il ricercatore vedrà un messaggio che lo informa di ripetere nuovamente la procedura di anonimizzazione e la successiva esportazione dei dati.
6. Analisi dei Dati	I dati anonimizzati sono utilizzati per scopi di ricerca nell'ambito dello studio PERICLE. L'analisi dei dati viene eseguita esclusivamente su questi dataset anonimizzati, che non contengono più alcuna informazione riconducibile ai singoli pazienti, per cui non sono soggetti a nessun tipo di restrizione regolatoria d'uso.

Quali sono le risorse di supporto ai dati?

Le risorse di supporto ai dati includono:

Un'applicazione locale fornita da AIMED per il caricamento e storage temporaneo (max 60 min.) dei dati pseudonimizzati e per la successiva anonimizzazione ed esportazione in un workspace su server cloud-based.

Il workspace server cloud è gestito da Google Cloud, un provider certificato che garantisce la conformità agli standard di sicurezza internazionali (ISO 27001, GDPR). Questo ambiente ospita i dati aggregati ed anonimizzati per l'analisi a livello centrale.

Le persone che gestiscono i dati, configurano i sistemi, e garantiscono la sicurezza dei processi.

- Personale IT: Responsabile della gestione tecnica delle infrastrutture, della manutenzione dei server, dei sistemi di sicurezza e del monitoraggio continuo delle reti.

- Ricercatori clinici: Il personale che raccoglie i dati pseudonimizzati e interagisce con i sistemi di raccolta e pseudonimizzazione.
- Amministratori di sistema: Responsabili della gestione degli accessi, della protezione dei dati e della sicurezza generale delle reti e dei server.
- Responsabili del trattamento dei dati: Individui incaricati di supervisionare la conformità alle normative sulla protezione dei dati (es. GDPR) e di garantire la sicurezza del trattamento.

Proporzionalità e Necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento dei dati nello studio PERICLE sono considerate specifiche, esplicite e legittime per i seguenti motivi:

1. Specifiche:
   - Lo scopo del trattamento è chiaramente definito: lo studio mira a valutare l'efficacia e la sicurezza del farmaco Clevidipina nel trattamento dell'ipertensione peri operatoria in pazienti sottoposti a chirurgia cardiovascolare. I dati raccolti sono utilizzati esclusivamente per questa specifica finalità medica e scientifica.
2. Esplicite:
   - Le finalità del trattamento sono chiaramente esplicitate nel protocollo dello studio e nella documentazione sottoposta alle autorità competenti. Il trattamento dei dati avviene in conformità con le normative applicabili, come l'Art. 110 del Codice Privacy italiano, che permette l'uso di dati senza consenso esplicito quando questo non è ottenibile, come nel caso di studi retrospettivi quali il PERICLE.
3. Legittime:
   - Le finalità del trattamento sono legittime in quanto perseguono un interesse per la ricerca scientifica nel campo medico, con l'obiettivo di migliorare le cure e la sicurezza dei pazienti. Il trattamento è condotto in conformità con la legge e con le misure di protezione della privacy previste per evitare qualsiasi rischio di violazione dei dati.

Quali sono le basi legali che rendono lecito il trattamento?

Nel contesto dello studio PERICLE, il trattamento dei dati personali senza richiedere il consenso dei pazienti trova le sue basi legali in diverse disposizioni normative. Di seguito sono presentate le principali basi legali che giustificano il trattamento dei dati nello studio:

1. Base legale (Art. 110 Codice Privacy Italiano):
    - L'Art. 110 del Codice Privacy Italiano, recentemente modificato, consente il trattamento dei dati personali a fini di ricerca scientifica senza il consenso del paziente, quando la raccolta del consenso è impossibile o comporterebbe un onere sproporzionato (come in studi retrospettivi). Lo studio PERICLE rientra in questa categoria, poiché prevede la raccolta di dati sanitari storici dai pazienti ricoverati in un reparto di rianimazione per cui sarebbe un onere sproporzionato per non dire infattibile rintracciarli per la raccolta del consenso.
2. Ricerca scientifica (Art. 9, par. 2, lett. j GDPR):
    - Il trattamento dei dati è giustificato perché necessario per finalità di ricerca scientifica o statistica, in conformità alle norme di legge e con garanzie adeguate. Nel caso dello studio PERICLE, i dati sanitari vengono raccolti e trattati esclusivamente per finalità scientifiche, rispettando le misure di sicurezza necessarie per proteggere la riservatezza dei pazienti.
3. Misure di sicurezza e minimizzazione dei rischi:
    - Sebbene il consenso non venga richiesto, sono state implementate rigorose misure di sicurezza per minimizzare i rischi di violazione dei dati, tra cui la pseudonimizzazione e la successiva anonimizzazione entro un tempo massimo di 60 minuti dall'inserimento dei dati. Queste misure sono in linea con quanto previsto dal GDPR per garantire la sicurezza dei dati personali trattati a fini scientifici.

In sintesi, il trattamento dei dati nello studio PERICLE si basa su solidi fondamenti legali ed all' interesse in ambito di ricerca scientifica e sanità, con adeguate garanzie di protezione della privacy.

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 nello studio PERICLE sono adeguati, pertinenti e limitati a quanto necessario per raggiungere le finalità del trattamento, conformemente al principio di minimizzazione dei dati previsto dal GDPR (Art. 5, par. 1, lett. c). Ogni tipo di dato raccolto è giustificato dall'esigenza di raggiungere gli obiettivi dello studio clinico in modo efficace e sicuro. Ecco una spiegazione dettagliata del perché ciascun dato previsto dal protocollo di studio è necessario:

1. Dati clinici sulla pressione sanguigna (pre, durante e post-operatoria):
    - Necessità: Lo studio mira a valutare l'efficacia dei farmaci nel controllo dell'ipertensione preoperatoria. Questi dati sono fondamentali per determinare le eventuali differenze tra i vari trattamenti somministrati in termini di efficacia nel ridurre e stabilizzare la pressione sanguigna nei pazienti.
    - Finalità: Valutare gli effetti del trattamento sul controllo dell'ipertensione, che è l'endpoint primario dello studio.
2. Parametri vitali (frequenza cardiaca, temperatura, saturazione di ossigeno):
    - Necessità: Questi dati sono necessari per monitorare lo stato di salute generale

del paziente durante il periodo peri operatorio e per verificare eventuali effetti collaterali dei farmaci somministrati.
Finalità: Verificare se i trattamenti somministrati hanno comportato rischi aggiuntivi per la salute del paziente e per monitorare eventuali variazioni fisiologiche che hanno potuto influenzare l'efficacia del trattamento.

3. Informazioni su complicanze post-operatorie (ad es. insufficienza renale, eventi avversi cardiaci, stroke):
    - Necessità: Le complicanze post-operatorie possono indicare una correlazione tra il trattamento e gli esiti clinici. Raccogliere questi dati consente di valutare la sicurezza del trattamento con Clevidipina rispetto agli altri farmaci.
    - Finalità: Valutare la sicurezza dei farmaci utilizzati, identificare potenziali effetti avversi e capire come la terapia impatta su questi esiti clinici.
4. Trattamenti precedenti e concomitanti:
    - Necessità: I trattamenti pregressi e concomitanti possono aver influito sulla risposta al trattamento e sulla sicurezza dei farmaci antiipertensivi. È importante sapere quali farmaci sono stati somministrati prima e durante il trattamento per escludere effetti confondenti.
    - Finalità: Assicurarsi che le differenze di risposta clinica non siano attribuibili ad altri trattamenti o farmaci.
5. Durata della degenza in terapia intensiva e tempi di recupero:
    - Necessità: La durata della degenza e il recupero post-operatorio forniscono informazioni cruciali sulla velocità di stabilizzazione del paziente e sugli effetti globali del trattamento sulla ripresa clinica.
    - Finalità: Misurare l'efficacia dei trattamenti in termini di stabilizzazione post-operatoria e recupero dei pazienti.
6. Eventuali eventi avversi (AEs e SAEs):
    - Necessità: Gli eventi avversi (AEs) e gli eventi avversi seri (SAEs) sono raccolti per monitorare la sicurezza dei farmaci somministrati. È essenziale sapere se e quando si sono verificati per valutare i rischi del trattamento.
    - Finalità: Garantire che il trattamento sia sicuro e che eventuali rischi siano identificati e quantificati.

Minimizzazione dei Dati.

- Ogni dato raccolto è strettamente pertinente e necessario per rispondere agli obiettivi primari e secondari dello studio, che includono la valutazione dell'efficacia e della sicurezza del trattamento per l'ipertensione peri operatoria.
- Non vengono raccolti dati non pertinenti, come informazioni personali che non influenzano lo studio, assicurando che i dati trattati siano limitati al minimo necessario per raggiungere le finalità.

In conclusione, i dati raccolti sono adeguati e pertinenti perché direttamente legati agli obiettivi clinici e scientifici dello studio, mentre la loro quantità e tipologia è limitata a ciò che è indispensabile per raggiungere tali finalità in modo efficiente e sicuro.

I dati sono esatti e aggiornati?

I dati che verranno raccolti sono retrospettivi e non devono essere pertanto aggiornati. Tuttavia, per garantire la qualità e l'accuratezza dei dati, vengono implementate diverse misure operative e tecniche di seguito descritte:

1. Raccolta Diretta dai Registri Ospedalieri:
    - Accuratezza: I dati vengono raccolti direttamente dalle cartelle cliniche ospedaliere, che contengono informazioni registrate da personale medico qualificato. Questo garantisce che le informazioni siano precise, in quanto basate su dati clinici ufficiali.
    - Aggiornamento: Poiché i dati provengono dai registri ufficiali, sono aggiornati riflettendo la storia clinica del paziente.
2. Pseudonimizzazione e Anonimizzazione Rapida:
    - Accuratezza nella Fase di Pre-Anonimizzazione: I medici ricercatori inseriscono i dati pseudonimizzati nell'applicativo AIMED che entro un massimo di 60 minuti vengono anonimizzati. Prima dell'anonimizzazione definitiva, i dati vengono revisionati manualmente dai medici ricercatori per confermare la correttezza delle informazioni inserite e correggere eventuali discrepanze. Durante questa fase, viene richiesto ai ricercatori la massima attenzione per evitare errori di trascrizione.
3. Controlli Automatici di Qualità sui Dati Inseriti:
   L'applicativo AIMED è progettato per rilevare eventuali discrepanze o anomalie nei dati inseriti, grazie a controlli automatici di coerenza e validità, che segnalano immediatamente errori potenziali. Questi controlli comprendono:

    - *Convalide incrociate dei campi*: per garantire che i campi correlati siano coerenti tra loro. Ad esempio, la data di dimissione del paziente deve essere successiva alla data di ammissione.
    - *Validazioni logiche*: per verificare che i dati logicamente correlati abbiano senso. Ad esempio, se un paziente è contrassegnato come deceduto, bisogna assicurarsi che ci sia una data di decesso corrispondente.
    - *Intervallo di età*: L'età del paziente deve essere compresa nei limiti previsti dal protocollo di studio.
    - *Segni vitali*: Pressione arteriosa, frequenza cardiaca e altri segni vitali devono rientrare in intervalli plausibili dal punto di vista medico.
    - *Valori di laboratorio*: I risultati di laboratorio devono rientrare in intervalli clinicamente accettabili e vengono segnalati per la revisione se non rientrano in tali intervalli.
    - *Formato della data*: per garantire che tutte le date siano nel formato AAAA-MM-GG.
    - *Formato numerico*: i valori numerici registrati verranno verificati se con i decimali appropriati dove richiesto.
    - *Formato testo*: i campi di testo (ad esempio, la definizione di AE) vengono verificati come limiti di caratteri specificati per evitare i caratteri proibiti.
    - *Campi obbligatori*: garantire che tutti i campi obbligatori (ad es. data di ammissione, data di dimissione, farmaco somministrato) siano compilati.

- *Completamento condizionale*: Verifica che i campi obbligatori condizionati siano compilati in base agli altri dati inseriti. Ad esempio, se un paziente viene contrassegnato come paziente che ha interrotto il farmaco antipertensivo a causa di una patologia, devono essere forniti i dettagli sulla patologia.

4. Formazione e Addestramento del Personale:
   - Il personale incaricato dell'inserimento e revisione dei dati è adeguatamente formato sulle procedure dello studio e sull'importanza di garantire la massima accuratezza e aggiornamento dei dati. Questa formazione riduce il rischio di errori umani durante il trattamento dei dati.

Qual è il periodo di conservazione dei dati?

Il periodo di conservazione dei dati nello studio PERICLE è determinato in funzione del tipo di dato (pseudonimizzato o anonimizzato), delle esigenze specifiche di ricerca e degli obblighi di legge applicabili.

- Dati personali pseudonimizzati (fase di pre-anonimizzazione): Questi dati saranno conservati solo per il tempo strettamente necessario all'anonimizzazione, cioè massimo 60 minuti. Una volta completata la fase di anonimizzazione, le informazioni personali vengono rimosse definitivamente dal sistema.
- Dati anonimizzati: Poiché lo scopo dello studio è la ricerca scientifica, i dati anonimizzati saranno conservati per un periodo di tempo più lungo, compatibilmente con la necessità di condurre analisi statistiche, verifiche scientifiche e potenziali follow-up della ricerca. Tuttavia, non essendo più considerati dati personali ai sensi del GDPR (poiché anonimizzati in modo irreversibile), non sono soggetti a limiti di conservazione specifici previsti per i dati personali. Il periodo di conservazione sarà generalmente di 5-10 anni, in linea con le prassi comuni per gli studi clinici, o per un periodo più lungo qualora richiesto da obblighi normativi o scientifici.

Giustificazione del Periodo di Conservazione.

1. Dati personali pseudonimizzati :
   - Necessità: Il limite massimo di 60 minuti per la conservazione dei dati personali non anonimizzati è giustificato dalla necessità di garantire che i dati siano prontamente anonimizzati per ridurre al minimo i rischi di violazione della privacy. Questo periodo è il minimo necessario per completare le operazioni tecniche e operative legate all'inserimento e alla pseudonimizzazione dei dati.
   - Finalità del trattamento: Questo breve periodo di conservazione è sufficiente a garantire l'efficacia del processo di anonimizzazione senza compromettere la riservatezza dei pazienti.

2. Dati anonimizzati:
    - Necessità: I dati anonimizzati sono essenziali per lo scopo dello studio, cioè l'analisi dell'efficacia e della sicurezza del farmaco Clevidipina. La conservazione di questi dati per un periodo necessario per completare l'analisi statistica, condurre eventuali approfondimenti scientifici successivi, e per rispondere a eventuali verifiche o richieste da parte delle autorità sanitarie.

In conclusione, il periodo di conservazione dei dati nello studio PERICLE è attentamente bilanciato per essere il minimo necessario al raggiungimento delle finalità scientifiche, senza eccedere rispetto a quanto richiesto. I dati personali vengono conservati solo fino al completamento del processo di anonimizzazione, mentre i dati anonimizzati, fondamentali per le analisi a lungo termine, sono conservati per un periodo compatibile con le esigenze di ricerca, salvo obblighi legali che impongano termini più lunghi.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Nel contesto dello studio PERICLE, gli interessati (ovvero i pazienti i cui dati vengono utilizzati) non vengono informati direttamente del trattamento dei loro dati e non viene richiesto il consenso, in conformità con quanto previsto dall'Art. 110 del Codice Privacy Italiano. Questo articolo consente l'utilizzo di dati personali a fini di ricerca scientifica senza il consenso esplicito quando l'informazione diretta degli interessati è impossibile o richiederebbe sforzi sproporzionati, come in studi retrospettivi basati su dati già esistenti.

Anche se non viene fornita una notifica diretta agli interessati, le informazioni relative allo studio saranno essere rese disponibili attraverso:

1. Pubblicazioni scientifiche: I risultati dello studio saranno pubblicati in riviste scientifiche e potranno includere informazioni generali sugli obiettivi dello studio e sulle modalità di trattamento dei dati, in forma anonima e aggregata.
2. Registro degli Studi Osservazionali (RSO), che raccoglie prospetticamente, in un unico archivio nazionale, i dati relative alle ricerche cliniche non interventistiche focalizzate sul farmaco. Le informazioni sullo studio PERICLE saranno inserite nel RSO garantendo la trasparenza delle finalità e delle modalità di trattamento dei dati.

Ove applicabile: come si ottiene il consenso degli interessati?

Non è previsto la richiesta del consenso degli interessati.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Non applicabile in quanti i dati sono anonimizzati.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Non applicabile.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Non applicabile.

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

In accordo a quanto previsto dal GDPR (Art. 28), ogni responsabile del trattamento ha delle responsabilità e compiti legati alla protezione dei dati. Tali obblighi vengono descritti in dettaglio nel contratto stipulato tra il titolare del trattamento (promotore dello studio) ed il responsabile del trattamento (AIMED).

Il contratto tra AIMED e il promotore dello studio include una clausola sulla protezione dei dati e sulla sicurezza, specificando gli obblighi di AIMED nella gestione dei dati personali per garantire che l'uso dei dati sia limitato agli scopi scientifici e che siano trattati in conformità alle normative sulla protezione dei dati. Di seguito le principali responsabilità:

- Implementazione delle misure tecniche per garantire la sicurezza dei dati (crittografia, accessi protetti, ecc.).
- Garantire il regolare funzionamento dell'applicativo durante il processo di anonimizzazione entro il limite di tempo di 60 minuti.
- Garantire che i dati personali non siano accessibili una volta completata l'anonimizzazione.
- Assicurare che i dati anonimi vengano trattati in modo conforme agli scopi della ricerca.
- Evitare qualsiasi tentativo di re identificazione dei dati.

- Mantenere misure di sicurezza adeguate durante l'elaborazione dei dati.
- Mantenimento della conformità con gli standard GDPR per la protezione dei dati.

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

I dati dello studio PERICLE non verranno trasferiti al di fuori dell'Unione Europea e comunque come già descritto in precedenza essendo anonimi non saranno soggetti a limitazioni regolatorie o legali per un loro eventuale trasferimento in paesi extra Europei.

Misure Esistenti o Pianificate

Crittografia.

Nel contesto dello studio PERICLE, il processo crittografico utilizza una funzione di hash crittografico (SHA-256) combinata con un "central salt" per proteggere gli identificatori dei

Una volta che l'identificatore originale del paziente è combinato con il salt, viene elaborato tramite una funzione di hash crittografico, come SHA-256. Questo algoritmo trasforma i dati in un hash, che è una stringa di lunghezza fissa, generalmente a 256 bit (32 byte), indipendentemente dalla dimensione dell'input.

L'hash generato è unidirezionale, il che significa che è impossibile risalire all'identificatore originale del paziente partendo dall'hash. Ciò garantisce che, anche se un malintenzionato riuscisse a ottenere l'hash, non potrebbe risalire al dato sensibile.

Vantaggi dell'uso di SHA-256 e del central salt:

- Sicurezza avanzata: SHA-256 è un algoritmo di hashing crittografico robusto e sicuro, largamente utilizzato per proteggere dati sensibili. La sua forza risiede nella complessità computazionale necessaria per invertire o prevedere l'hash.
- Protezione contro collisioni: Grazie all'uso di un salt unico e all'algoritmo SHA-256, la probabilità che due pazienti diversi generino lo stesso hash (collisione) è estremamente ridotta.
- Prevenzione di attacchi basati su hash pre-computati: L'uso del salt garantisce che gli attacchi come il rainbow table, che si basano su pre-calcoli di hash comuni, siano inefficaci, in quanto l'aggiunta di un salt genera un hash unico per ogni paziente.

L'uso di SHA-256 combinato con un central salt fornisce una soluzione sicura per gestire gli identificatori dei pazienti. Questo approccio garantisce che gli identificatori personali siano

protetti durante il processo di pseudonimizzazione, assicurando al contempo che i dati possano essere utilizzati per scopi scientifici senza compromettere la privacy dei pazienti.

Anonimizzazione.

Gli identificatori dei dati pseudonimizzati vengono combinati con un salt centrale e successivamente elaborati tramite una funzione di hash crittografico (SHA-256). Questo passaggio garantisce che l'identificatore del paziente non possa essere invertito o ricostruito da eventuali malintenzionati.
Il processo di anonimizzazione deve essere completato entro 60 minuti dall'inserimento dei dati nel sistema. Dopo questo periodo, i dati risultano completamente anonimi e non possono essere ricondotti ai singoli pazienti, né attraverso i ricercatori né tramite altre fonti.

Controllo degli Accessi Logici.

I profili utente sono definiti in base al ruolo specifico e alle responsabilità di ciascun partecipante allo studio. Questo principio di "least privilege" garantisce che gli utenti abbiano accesso solo alle informazioni strettamente necessarie per svolgere i loro compiti.

- Esistono vari livelli di accesso, come:
    - Ricercatori clinici: Accesso limitato ai dati necessari per l'inserimento e l' anomizzazione.
    - Amministratori di sistema: Accesso ai sistemi per la gestione tecnica, senza visibilità sui dati.
    - Analisti di dati: Accesso ai dati anonimizzati per finalità di analisi e ricerca scientifica, senza possibilità di collegare i dati ai pazienti.

Attribuzione dei Profili Utente.

I profili utente vengono attribuiti tramite un processo formale, che include:

- Configurazione dei permessi: Ogni utente riceve un set specifico di permessi, configurato in base alle sue mansioni. I permessi sono gestiti tramite un sistema di ruoli predefiniti, che limita l'accesso a determinati dati o funzionalità dell'applicativo.
- Autenticazione a più fattori (MFA): L'accesso ai dati sensibili richiede l'autenticazione tramite password sicure ed un secondo fattore di autenticazione (codice inviato al cellulare), per aumentare il livello di sicurezza.

Monitoraggio e Revisione degli Accessi.

- Log di accesso: Ogni accesso al sistema è registrato in un log di controllo, che monitora chi ha effettuato l'accesso, quando e quali azioni sono state eseguite. Questo log è utile per rilevare accessi non autorizzati o comportamenti sospetti.
- Revisione periodica dei permessi: I profili e i permessi degli utenti vengono rivisti periodicamente per assicurarsi che siano allineati alle esigenze operative. Se un utente non necessita più di determinati permessi, questi vengono revocati.

Gestione delle Credenziali.

- Le credenziali di accesso sono gestite in modo sicuro. Gli utenti sono tenuti a cambiare le password a intervalli regolari e le password devono rispettare standard di complessità (lunghezza minima, uso di caratteri speciali, ecc.).
- In caso di cessazione della partecipazione o del progetto, le credenziali degli utenti vengono immediatamente disabilitate per evitare accessi non autorizzati.

Tracciabilità.

Tutti gli eventi significativi relativi all'accesso ai dati, alla modifica dei record e ad altre operazioni sensibili vengono tracciati tramite un sistema di log. Gli eventi tracciati includono:

  - Accesso ai dati (quando e da chi).
  - Modifica o inserimento di dati (che dati sono stati cambiati e da chi).
  - Tentativi di accesso non autorizzato o fallito.
  - Eventuali esportazioni o copie di dati.
  - Modifiche ai permessi di accesso degli utenti.
- Il sistema registra dettagli come:
  - Identificativo dell'utente: Chi ha eseguito l'azione.
  - Timestamp: Data e ora dell'evento.
  - Descrizione dell'attività: Tipo di operazione effettuata (es. accesso, modifica, esportazione).
  - Esito dell'operazione: Se l'azione è stata eseguita con successo o se ci sono stati errori o tentativi falliti.

Conservazione delle Registrazioni (Log).

- I log di tracciabilità sono conservati per un periodo di tempo sufficiente a garantire la conformità alle normative e per soddisfare eventuali richieste di audit o verifiche e comunque per un periodo di almeno cinque anni, in linea con le prassi di ricerca clinica e le linee guida di sicurezza.

Monitoraggio e Revisione dei Log.

- I log vengono monitorati attivamente per rilevare comportamenti sospetti o accessi non autorizzati. Questo monitoraggio è supportato da strumenti automatici che segnalano anomalie o eventi fuori norma.
- Viene effettuata una revisione periodica dei log per garantire la sicurezza e l'integrità dei dati trattati.

Sicurezza delle Registrazioni.

- I log di tracciabilità sono conservati in forma crittografata e accessibili solo al personale autorizzato. Le registrazioni non possono essere modificate, garantendo l'integrità e l'affidabilità dei dati di tracciabilità.
- Le registrazioni sono soggette a backup regolari per evitare perdite accidentali e per garantire che siano sempre disponibili in caso di audit o richieste delle autorità.

Minimizzazione dei Dati.

- Vengono raccolti solo i dati strettamente necessari per gli scopi dello studio e vengono evitati dati identificativi come il nome, l'indirizzo o il codice fiscale, che non sono rilevanti per la ricerca.
  Dati sensibili come l'età esatta o le date specifiche (come la data di nascita) possono essere aggregati o approssimati (ad es., l'età del paziente può essere raggruppata per fasce) per ridurre ulteriormente il rischio di identificazione.
- Gli identificatori univoci dei pazienti, sono poi trattati attraverso un processo di hashing crittografico combinato con un salt che trasforma l'identificatore in una stringa unica, impedendo qualsiasi ricostruzione dell'identificatore originale.
  Questo processo rende impossibile risalire ai dati originali anche in caso di accesso non autorizzato ai dati pseudonimizzati.
- Solo il personale strettamente necessario per il processo di raccolta, pseudonimizzazione e anonimizzazione ha accesso ai dati personali non anonimizzati. Dopo l'anonimizzazione, l'accesso ai dati è ulteriormente limitato solo al personale che analizza i dati per scopi di ricerca, e comunque questi dati non possono essere ricondotti ai pazienti.
- Tutti gli accessi ai dati vengono tracciati, garantendo che l'accesso non autorizzato possa essere individuato e prevenuto.
- Durante la trasmissione e la conservazione, i dati pseudonimizzati sono protetti tramite crittografia avanzata. Anche se i dati venissero intercettati durante la trasmissione o fossero soggetti a una violazione di sicurezza, la crittografia impedirebbe che fossero leggibili o utilizzabili.

Vulnerabilità.

La gestione delle vulnerabilità legata ai software impiegati è una priorità, ed è garantita come segue:

- Patch Management: attraverso un sistema di gestione delle patch che garantisce l'installazione tempestiva di aggiornamenti e patch di sicurezza rilasciate dai fornitori dei software. Questo processo è automatizzato, ove possibile, per ridurre i rischi di vulnerabilità note.
- Aggiornamenti automatici: I software critici utilizzati nello studio, inclusi quelli per la gestione dei dati e per l'anonimizzazione, sono configurati per ricevere aggiornamenti automatici. Questo assicura che tutte le ultime correzioni di sicurezza siano applicate senza ritardi.

Strumenti di Vulnerability Scanning.

- Vengono utilizzati strumenti di scansione delle vulnerabilità per identificare eventuali falle nei software o nelle configurazioni di sistema. Questi strumenti eseguono

  scansioni regolari e automatiche per rilevare vulnerabilità note (come CVE - Common Vulnerabilities and Exposures) e segnalano potenziali minacce agli amministratori di sistema.

Strumenti di Monitoraggio della Sicurezza.

- I sistemi software sono monitorati tramite strumenti di Security Information and Event Management (SIEM), che raccolgono e analizzano in tempo reale i log e le attività di rete per individuare anomalie o potenziali tentativi di sfruttare vulnerabilità.
- Questo monitoraggio consente di intervenire rapidamente in caso di tentativi di attacco o anomalie di sicurezza.

Firewall e Sistemi di Intrusion Detection/Prevention (IDS/IPS).

- I software e i sistemi utilizzati nello studio sono protetti da firewall e da sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), che monitorano il traffico di rete in tempo reale e bloccano eventuali tentativi di accesso non autorizzato o attacchi basati su vulnerabilità note.
- Gli IDS/IPS analizzano il traffico in ingresso e in uscita per individuare comportamenti sospetti, garantendo una protezione proattiva contro possibili minacce.

Controllo e Verifica dei Software.

- Prima di essere impiegati nello studio, tutti i software vengono sottoposti a valutazione di sicurezza per garantire che non presentino vulnerabilità note e che siano conformi agli standard di sicurezza richiesti.
- Questa verifica include controlli sulle versioni del software, validazione delle firme digitali degli aggiornamenti e confronto con elenchi di vulnerabilità conosciute.

Lotta contro il Malware.

Nel contesto dello studio PERICLE, il momento a rischio si verifica quando il ricercatore esce dalla rete interna ospedaliera per effettuare il trasferimento dei dati anonimizzati verso un workspace cloud-based esterno. Questo workspace raccoglie i dati anonimi provenienti da tutti i centri coinvolti nello studio e li aggrega nel database centrale. Per garantire la sicurezza durante questo trasferimento, sono implementate le seguenti misure di protezione contro il malware e per mantenere l'integrità dei dati:

- Durante il trasferimento, i dati anonimizzati vengono crittografati con standard avanzati (come AES-256). La crittografia end-to-end garantisce che i dati non possano essere letti da terze parti durante la trasmissione, nemmeno se il traffico venisse intercettato. Il ricercatore utilizza una connessione sicura HTTPS per accedere al workspace cloud.
- Il firewall dell'ospedale e del workspace cloud-based è configurato per filtrare il traffico in entrata e in uscita, consentendo solo le connessioni autorizzate per il trasferimento dei dati. Qualsiasi traffico anomalo o sospetto viene bloccato. Inoltre, vengono implementati controlli specifici per malware all'interno del firewall per garantire che il trasferimento avvenga in modo sicuro.
- Prima del trasferimento, viene eseguito un controllo di integrità sui dati anonimizzati per garantire che non siano stati alterati o contaminati da malware. All'arrivo nel workspace cloud, un altro controllo di integrità verifica che i dati ricevuti siano identici a quelli inviati.
  Questo processo utilizza hash crittografici (come SHA-256) per garantire che i dati non siano stati modificati durante il trasferimento.
- L'accesso al workspace cloud da parte del ricercatore richiede una autenticazione multi-fattore (MFA), che aggiunge un ulteriore livello di sicurezza. Questo riduce il rischio che un attaccante possa accedere al sistema, anche in caso di compromissione delle credenziali del ricercatore
- L'accesso al workspace cloud è limitato solo a ricercatori autorizzati, e ogni accesso viene monitorato e registrato. I log di accesso permettono di rilevare eventuali anomalie o tentativi di accesso non autorizzato.

Sicurezza dei Siti Web.

- Il sito web dove verrano caricati i dati anonimizzati, utilizza una connessione HTTPS sicura con certificati SSL/TLS aggiornati. Questo garantisce che tutti i dati trasmessi tra il browser del ricercatore e il server siano crittografati e protetti da intercettazioni o attacchi "man-in-the-middle".
- Viene implementata una crittografia avanzata (AES-256) per proteggere le comunicazioni, assicurando che anche se i dati venissero intercettati, non sarebbero leggibili senza la chiave di decrittazione.
- L'accesso al sito web è protetto da un sistema di autenticazione multi-fattore (MFA). Oltre alla password, gli utenti devono fornire un secondo fattore di autenticazione, cioè un codice inviato via SMS. Questo riduce significativamente il rischio di accesso non autorizzato, anche in caso di furto delle credenziali.
- Ogni attività sul sito web viene monitorata e registrata tramite un sistema di logging. Questo include informazioni su chi ha effettuato l'accesso, quali operazioni sono state eseguite, e quali file sono stati caricati.
- Il monitoraggio avviene in tempo reale attraverso un Security Information and Event Management (SIEM), che analizza i log alla ricerca di comportamenti sospetti o anomali e genera avvisi automatici in caso di potenziali minacce.
- Il sito web e i suoi componenti (inclusi i server, i database, e il software applicativo) vengono costantemente aggiornati con le ultime patch di sicurezza. Un sistema di patch management garantisce che tutte le vulnerabilità conosciute siano risolte tempestivamente.
- Oltre alla crittografia durante la trasmissione, i dati caricati sul sito web vengono crittografati a riposo sui server. Questo garantisce che, anche in caso di violazione fisica del server o del disco, i dati anonimi rimangano protetti e non leggibili senza la chiave di decrittazione.

Backup.

I backup saranno conservati esclusivamente nel cloud e non in forma fisica offline. Di seguito sono descritti i metodi e le misure implementate per gestire e proteggere i backup cloud-based.

- Tutti i backup archiviati nel cloud sono crittografati utilizzando algoritmi avanzati come AES-256. La crittografia garantisce che i dati siano protetti sia durante la trasmissione che durante l'archiviazione nel cloud, impedendo che possano essere letti da terze parti non autorizzate.
- Le chiavi di crittografia sono gestite in modo sicuro e l'accesso ad esse è limitato al personale autorizzato. Viene implementato un sistema di rotazione regolare delle chiavi per ridurre il rischio di compromissione.
- I backup cloud-based sono soggetti a replicazione geografica in data center diversi, situati in aree geografiche distinte, per garantire la disponibilità dei dati anche in caso di disastri che possano compromettere uno dei data center.
- Questo sistema di ridondanza protegge contro la perdita di dati e assicura che i dati siano sempre accessibili e ripristinabili, riducendo il rischio di down time.
- L'accesso ai backup cloud-base è strettamente controllato tramite un sistema di autenticazione forte, come l'autenticazione multi-fattore (MFA). Solo il personale autorizzato ha accesso ai backup e il sistema di controllo degli accessi basato su ruoli

(RBAC) garantisce che ogni utente possa accedere solo alle risorse necessarie per le proprie attività.
- Ogni accesso viene monitorato e registrato per garantire la tracciabilità e l'identificazione di eventuali accessi non autorizzati o comportamenti sospetti.
- Il sistema cloud utilizzato per i backup è protetto contro malware e ransomware grazie a strumenti di sicurezza integrati che rilevano e bloccano attività sospette o tentativi di modifica non autorizzata dei file di backup.
- Il provider cloud scelto per il backup è conforme agli standard di sicurezza e protezione dei dati (come ISO/IEC 27001 e GDPR). Questo garantisce che i dati anonimizzati siano trattati secondo le normative vigenti e che le misure di sicurezza siano continuamente verificate e aggiornate.

Contratto con il Responsabile del Trattamento.

Il contratto stabilisce che il responsabile del trattamento deve trattare i dati personali in conformità con il GDPR, il Codice Privacy Italiano e tutte le altre normative applicabili in materia di protezione dei dati. Questo include l'adozione di tutte le misure di sicurezza tecniche e organizzative necessarie per proteggere i dati personali.

Il contratto specifica le misure di sicurezza tecniche e organizzative che il responsabile del trattamento è obbligato a implementare per garantire la protezione dei dati. Queste misure includono, a titolo esemplificativo:

- Crittografia dei dati durante la trasmissione e l'archiviazione.
- Controllo rigoroso degli accessi (inclusi autenticazione multi-fattore, gestione delle credenziali e sistemi di logging).
- Protezione contro malware e attacchi informatici
- Politiche di backup sicuri e meccanismi di ripristino per garantire la disponibilità dei dati.
- È previsto un obbligo di notifica tempestiva in caso di violazioni di sicurezza. Il responsabile deve informare il titolare del trattamento senza ritardi ingiustificati, entro un tempo massimo definito nel contratto (generalmente 24-72 ore), in caso di violazione dei dati personali che potrebbe comportare un rischio per i diritti e le libertà degli interessati.
- È prevista la possibilità per il titolare del trattamento (promotore dello studio) di effettuare audit e verifiche periodiche sulle misure di sicurezza adottate dal responsabile.
- Qualora il responsabile deleghi alcune attività ad un sub-responsabile, il responsabile deve garantire che il sub-responsabile adotti le stesse misure di sicurezza e segua gli stessi obblighi definiti nel contratto principale.
- Il responsabile del trattamento può trattare i dati personali esclusivamente per le finalità specifiche definite dal titolare del trattamento e deve seguire le istruzioni documentate del titolare.

- L'accesso ai dati deve essere limitato solo al personale autorizzato che necessiti di accedere ai dati per svolgere le loro mansioni e che sia stato formato adeguatamente in materia di protezione dei dati.
- Vengono specificate le procedure da seguire in caso di data breach, compreso un piano di risposta agli incidenti. Il responsabile deve fornire dettagli sulle azioni correttive che verranno intraprese per mitigare l'impatto della violazione e prevenire future compromissioni. Inoltre, il responsabile del trattamento deve cooperare con il titolare per garantire che vengano soddisfatti i requisiti di notifica alle autorità competenti e agli interessati.

Sicurezza dei Canali Informatici.

Tutte le comunicazioni attraverso la rete avvengono tramite canali crittografati, utilizzando protocollo HTTPS con certificati SSL/TLS per la crittografia end-to-end. Questo garantisce che i dati siano protetti da intercettazioni mentre vengono trasmessi dal centro al database dello studio sul workspace cloud-based.

La rete sulla quale avviene il trattamento è protetta da firewall di rete avanzati, che monitorano il traffico in entrata e in uscita, bloccando qualsiasi attività non autorizzata o sospetta.

L'accesso alla rete e ai sistemi dove il trattamento dei dati avviene è protetto da autenticazione multi-fattore (MFA). Oltre alla password, gli utenti devono fornire un secondo fattore di autenticazione. Questo aggiunge un ulteriore livello di protezione, riducendo il rischio di compromissione delle credenziali e prevenendo accessi non autorizzati anche in caso di furto della password.

Tutte le attività di accesso alla rete e ai dati vengono registrate tramite un sistema di logging centralizzato. I log includono informazioni dettagliate su chi ha effettuato l'accesso, quando, da dove, e quali operazioni sono state eseguite.

I sistemi di rete e i dispositivi utilizzati per il trattamento dei dati sono costantemente aggiornati con le patch di sicurezza più recenti. Viene implementato un processo di patch management automatizzato per garantire che tutte le vulnerabilità conosciute siano tempestivamente risolte.

Sicurezza dell'Hardware.

Il cloud-based server su cui vengono raccolti i dati anonimizzati dei vari centri è gestito da Google Cloud, un fornitore qualificato e certificato, che aderisce ai più elevati standard di sicurezza del mercato. Questo include la conformità a standard internazionali come:

- ISO/IEC 27001: Gestione della sicurezza delle informazioni.
- ISO/IEC 27017: Sicurezza nel cloud.
- ISO/IEC 27018: Protezione dei dati personali nel cloud.

- SOC 1/2/3: I rapporti SOC (System and Organization Controls) sono rapporti di audit di terzi indipendenti. e riguardano controlli sulla rendicontazione finanziaria, controlli su sicurezza, disponibilità, integrità dell'elaborazione, riservatezza e privacy.
- GDPR: Regolamento generale sulla protezione dei dati per la conformità alle normative europee.

L'uso di un fornitore di questa portata assicura che l'infrastruttura cloud sia protetta da misure avanzate di sicurezza fisica e digitale, riducendo i rischi legati a violazioni di dati e garantendo un alto livello di affidabilità per la raccolta e l'archiviazione sicura dei dati anonimizzati.

Prevenzione delle Fonti di Rischio.

Ecco le principali strategie impiegate per prevenire rischi di carattere generale:

- Crittografia durante la trasmissione: Tutte le comunicazioni di dati tra server e dispositivi sono protette tramite crittografia SSL/TLS (HTTPS), garantendo che i dati non possano essere intercettati durante il trasferimento.
- Crittografia dei dati a riposo: I dati, inclusi quelli anonimizzati, sono crittografati a livello di archiviazione utilizzando standard come AES-256. Anche in caso di accesso non autorizzato ai server o dispositivi di archiviazione, i dati rimangono protetti.
- Per accedere ai sistemi critici, gli utenti devono autenticarsi utilizzando autenticazione multi-fattore (MFA). Questo riduce significativamente il rischio di compromissione delle credenziali, poiché richiede non solo una password, ma anche un secondo fattore come un codice univoco generato tramite un'applicazione mobile o un dispositivo hardware.
- Viene implementato un sistema di monitoraggio continuo che registra tutte le attività degli utenti e dei sistemi, inclusi accessi, modifiche ai dati, e tentativi di violazione.
- I log di sistema sono conservati per garantire la tracciabilità e sono regolarmente analizzati per prevenire e rispondere a potenziali rischi.
- Le reti e i server sono protetti da firewall avanzati che filtrano il traffico di rete per bloccare connessioni non autorizzate o sospette. I sistemi di prevenzione delle intrusioni (IPS) monitorano continuamente il traffico di rete per rilevare e bloccare attività dannose come malware o tentativi di intrusione.
- I dati vengono sottoposti a backup regolari nel cloud per prevenire la perdita di informazioni in caso di incidenti, errori umani, o attacchi informatici come ransomware. I backup sono criptati e archiviati in più località geografiche per garantire che i dati siano sempre disponibili e sicuri.
- Tutti i software, server e sistemi operativi utilizzati nello studio sono regolarmente aggiornati per includere le ultime patch di sicurezza. Questo riduce la probabilità che vulnerabilità note possano essere sfruttate da attori malintenzionati.
- Per quanto riguarda i centri clinici, la sicurezza fisica e informatica è gestita secondo le politiche di sicurezza delle istituzioni a cui appartengono, che includono protezione fisica degli edifici, controllo degli accessi, videosorveglianza, e sicurezza delle postazioni di lavoro.

Gestire gli Incidenti di Sicurezza e le Violazioni dei Dati Personali.

Poiché i dati trasferiti nel cloud-based workspace dai vari centri sono già anonimizzati, eventuali rischi si concentrano principalmente nella fase di acquisizione dei dati pseudonimizzati prima della loro de-identificazione. Ecco i processi chiave per gestire questi eventi:

- Crittografia dei dati pseudonimizzati: I dati pseudonimizzati vengono crittografati a livello locale, già prima del loro trasferimento al cloud-based workspace, utilizzando tecnologie avanzate (come AES-256). Questo garantisce che i dati siano protetti anche se dovesse verificarsi una violazione a livello del centro.
- Controllo degli accessi: L'accesso ai dati pseudonimizzati è rigorosamente limitato al personale autorizzato attraverso l'uso di autenticazione multi-fattore (MFA) e controllo degli accessi basato su ruoli (RBAC). Ogni accesso viene monitorato e registrato nei log.
- Politiche di sicurezza nei centri clinici: Le istituzioni cliniche che partecipano allo studio implementano di default delle loro politiche di sicurezza specifiche che includono misure per la protezione fisica e logica dei dati clinici sensibili, riducendo il rischio di compromissioni durante la fase di acquisizione.

In caso di violazione o sospetto di incidente di sicurezza, vengono attivate le seguenti procedure operative:

- Notifica immediata: Se si rileva una violazione dei dati personali pseudonimizzati, il responsabile della sicurezza del centro clinico deve informare immediatamente il titolare del trattamento. La notifica deve includere dettagli sugli eventi, i dati potenzialmente compromessi e le azioni intraprese per contenere la violazione.
- Valutazione del rischio: Viene eseguita una valutazione dell'impatto della violazione, per stabilire se l'incidente possa comportare rischi per i diritti e le libertà degli interessati. Nel caso dei dati pseudonimizzati, il rischio è ridotto, ma sarà comunque eseguita una valutazione del possibile impatto.
- Misure di contenimento: Il personale di sicurezza attiva immediatamente misure di contenimento per isolare il sistema compromesso, bloccare gli accessi non autorizzati e impedire ulteriori compromissioni. Viene avviata una analisi per determinare l'origine dell'attacco e identificare le eventuali falle di sicurezza.
- Se la violazione riguarda i dati pseudonimizzati e comporta rischi elevati per i diritti degli interessati, viene seguita la procedura di notifica alle autorità competenti (DPO locale e Garante della Privacy), come richiesto dal GDPR, entro 72 ore dal rilevamento.
- Gli interessati vengono notificati solo se esiste un rischio concreto che la violazione possa compromettere la loro privacy o sicurezza, anche se il rischio è mitigato dalla pseudonimizzazione dei dati.
- Dopo aver contenuto la violazione, viene attuato un piano di ripristino della sicurezza che comprende:
    - La verifica e ripristino dei sistemi compromessi.
    - L'implementazione di ulteriori misure di sicurezza per prevenire incidenti futuri, come aggiornamenti delle patch o rafforzamento dei controlli di accesso.
    - La conduzione di un audit post-incident per identificare le cause principali e le aree di miglioramento.

Accesso Illegittimo ai Dati

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

Qualora le informazioni pseudonimizzate venissero combinate con altre fonti di dati esterne, come i codici pseudonimizzati, l'impatto è la re-identificazione che potrebbe portare alla violazione della privacy degli interessati, rivelando informazioni personali e dati sensibili relativi alla loro condizione medica.
Se il rischio di violazione dei dati pseudonimizzati si concretizzasse, i principali impatti sugli interessati includerebbero la re-identificazione e l'esposizione dei dati sanitari sensibili, con conseguenti danni alla privacy, alla reputazione, e alla vita emotiva e sociale.

In casi estremi si potrebbe anche realizzare un furto di identità per scopi illeciti. Le misure di sicurezza pianificate (come crittografia, MFA, e controllo degli accessi) mirano a mitigare questi impatti, ma resta una certa vulnerabilità durante la fase antecedente all'anonimizzazione. Va tuttavia sottolineato che questo tipo di violazione non comporterebbe comunque effetti sulle condizioni cliniche del paziente né sugli eventuali futuri trattamenti terapeutici.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Le principali minacce che potrebbero concretizzare il rischio durante la fase di acquisizione dei dati pseudonimizzati, prima della loro anonimizzazione, riguardano diversi tipi di attacchi e vulnerabilità che potrebbero compromettere la sicurezza dei dati. Ecco alcune delle minacce più rilevanti: Phishing, Accesso non autorizzato, Malware e Ransoware ed eventuali minacce interne (Insider Threats).

Quali sono le fonti di rischio?

Le fonti di rischio che potrebbero compromettere la sicurezza dei dati pseudonimizzati, prima della loro anonimizzazione, provengono da vari ambiti e includono vulnerabilità tecnologiche, errori umani, attacchi esterni e interni.
Di seguito sono elencate le principali possibili fonti di rischio:

- Errori umani quali uso improprio delle credenziali di accesso, errori di inserimento dati, mancato rispetto delle procedure di sicurezza, o invio accidentale di informazioni a destinatari sbagliati.

• Attacchi informatici da parte di hacker o organizzazioni malintenzionate quali Phishing, Malware o Ransomware.
• Minacce interne possono provenire da dipendenti, collaboratori o fornitori che hanno accesso ai dati pseudonimizzati e che, intenzionalmente o accidentalmente, compromettono la loro sicurezza.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Crittografia,
- Anonimizzazione,
- Controllo degli accessi logici,
- Tracciabilità,
- Minimizzazione dei dati,
- Vulnerabilità,
- Lotta contro il malware,
- Sicurezza dei siti web,
- Backup,
- Contratto con il responsabile del trattamento,
- Sicurezza dei canali informatici,
- Sicurezza dell'hardware,
- Prevenzione delle fonti di rischio,
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali.

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

Limitata

La giustificazione per considerare la gravità del rischio di violazione della privacy nella fase antecedente l'anonimizzazione dei dati come limitata si basa sui seguenti elementi:

1. Pseudonimizzazione dei Dati

- I dati trattati nella fase antecedente all'anonimizzazione sono già pseudonimizzati, il che significa che le informazioni identificative dirette sono state rimosse o sostituite da codici. La pseudonimizzazione, pur non essendo irreversibile, rappresenta una misura importante di protezione, in quanto rende più difficile identificare gli interessati senza informazioni aggiuntive. Anche in caso di violazione, sarebbe necessario un ulteriore collegamento a dati esterni per consentire la re-identificazione. Questo riduce significativamente il rischio di danno diretto per gli interessati.

2. Crittografia durante la Trasmissione e l'Archiviazione

- I dati pseudonimizzati sono protetti attraverso crittografia avanzata sia durante la trasmissione che nell'archiviazione locale, nei centri clinici e nei sistemi cloud. Ciò garantisce che i dati non possano essere letti o utilizzati in caso di violazione fisica o digitale. Anche se i dati venissero intercettati o rubati durante la trasmissione, sarebbero illeggibili senza la chiave di decrittazione, riducendo drasticamente l'impatto di una potenziale violazione.

3. Accesso Limitato e Controllato

- L'accesso controllato ai dati pseudonimizzati e sistemi di autenticazione multi-fattore (MFA), assicurano che solo il personale autorizzato possa accedere ai dati. Inoltre, ogni accesso viene monitorato e tracciato. Anche in caso di incidente, la violazione sarebbe circoscritta e facilmente identificabile.

4. Riduzione della Finestra di Esposizione

· La fase di acquisizione dei dati pseudonimizzati è temporanea e limitata nel tempo. I dati vengono anonimizzati entro un breve lasso di tempo (entro un massimo di 60 minuti dall'acquisizione), riducendo il periodo in cui i dati pseudonimizzati sono esposti a potenziali rischi, limitando così la probabilità di una violazione.

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

Trascurabile/Limitata,

Nel contesto dello studio PERICLE le minacce principali, come phishing, malware, accessi non autorizzati e vulnerabilità di sistema, possono essere considerate trascurabili/limitate. L'efficacia delle misure implementate quali l'autenticazione multifattoriale (MFA), sicurezza, i sistemi di prevenzione delle intrusioni (IPS), la crittografia dei dati e la formazione del personale dello studio, gioca un ruolo cruciale nel ridurre la probabilità che queste minacce abbiano successo.

Modifiche Indesiderate dei Dati

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

Se il rischio di violazione dei dati pseudonimizzati si concretizzasse, i principali impatti sugli interessati includerebbero la re-identificazione e l'esposizione dei dati sanitari sensibili, con conseguenti danni alla privacy, alla reputazione, e alla vita emotiva e sociale. In casi estremi si potrebbe anche realizzare un furto di identità per scopi illeciti. Le misure di sicurezza pianificate (come crittografia, MFA, e controllo degli accessi) mirano a mitigare questi impatti, ma resta una certa vulnerabilità durante la fase antecedente all'anonimizzazione. Va tuttavia sottolineato che questo tipo di violazione non comporterebbe comunque effetti sulle condizioni cliniche del paziente né sugli eventuali trattamenti terapeutici.

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

Le principali minacce che potrebbero consentire la concretizzazione del rischio includono phishing, malware, accesso non autorizzato, e vulnerabilità di sistema. Anche l'errore umano, le minacce interne, e il furto di dispositivi rappresentano potenziali fonti di rischio. Queste minacce possono essere mitigate attraverso l'implementazione di misure di sicurezza avanzate come la crittografia, l'autenticazione multi-fattore, l'aggiornamento costante dei sistemi e la formazione del personale.

Quali sono le fonti di rischio?

Le fonti di rischio principali includono l’errore umano, gli attacchi informatici quali phishing, malware e ransomware, infrastrutture IT inadeguate, e vulnerabilità di sistema.

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

Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Backup, Lotta contro il malware, Contratto con il responsabile del trattamento, Sicurezza dei siti web, Sicurezza dei canali informatici, Vulnerabilità, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Prevenzione delle fonti di rischio.

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

Limitata.

La gravità del rischio è stata definita limitata per diverse ragioni. Le misure di sicurezza pianificate, come la pseudonimizzazione, la crittografia, il controllo degli accessi, e la prevenzione delle intrusioni, riducono significativamente la probabilità di una violazione riuscita e mitigano l'impatto potenziale sugli interessati. Inoltre, la rapida transizione dei dati dall'essere pseudonimizzati a completamente anonimi e la conformità alle normative internazionali rafforzano ulteriormente questa valutazione. Anche in caso di violazione, gli impatti potenziali sarebbero limitati grazie alla protezione multilivello offerta dalle misure pianificate.

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

Limitata,

La probabilità del rischio è stata definita come limitata per diversi motivi. Le misure di sicurezza implementate, come la crittografia, l'autenticazione multi-fattore, il controllo degli accessi, il monitoraggio continuo e la prevenzione delle intrusioni, gli aggiornamenti e la gestione delle patch di sicurezza e la formazione del personale, riducono notevolmente la possibilità che le minacce identificate possano concretizzarsi.

Inoltre, l'uso di cloud provider certificati e conformi agli standard di sicurezza e la riduzione della finestra di esposizione dei dati pseudonimizzati minimizzano ulteriormente il rischio.

Anche in presenza di attacchi, le difese multilivello riducono la probabilità di successo, limitando il rischio complessivo a un livello gestibile.

Perdita di dati

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

Qualora le informazioni pseudonimizzate venissero combinate con altre fonti di dati esterne, come i codici pseudonimizzati, l'impatto è la re-identificazione che potrebbe portare alla violazione della privacy degli interessati, rivelando informazioni personali e dati sensibili relativi alla loro condizione medica.

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

Le principali minacce che potrebbero consentire la concretizzazione del rischio includono phishing, malware, accesso non autorizzato, e vulnerabilità di sistema. Anche l'errore umano, le minacce interne, e il furto di dispositivi rappresentano potenziali fonti di rischio. Queste minacce possono essere mitigate attraverso l'implementazione di misure di sicurezza avanzate come la crittografia, l'autenticazione multi-fattore, l'aggiornamento costante dei sistemi e la formazione del personale.

Quali sono le fonti di rischio?

Le fonti di rischio che potrebbero compromettere la sicurezza dei dati pseudonimizzati, prima della loro anonimizzazione, provengono da vari ambiti e includono vulnerabilità tecnologiche, errori umani, attacchi esterni e interni. Di seguito sono elencate le principali possibili fonti di rischio:
• Errori umani quali uso improprio delle credenziali di accesso, errori di inserimento dati, mancato rispetto delle procedure di sicurezza, o invio accidentale di informazioni a destinatari sbagliati.
• Attacchi informatici da parte di hacker o organizzazioni malintenzionate quali Phishing, Malware o Ransomware.
• Minacce interne possono provenire da dipendenti, collaboratori o fornitori che hanno accesso ai dati pseudonimizzati e che, intenzionalmente o accidentalmente, compromettono la loro sicurezza.

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

Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Sicurezza dei siti web, Backup, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Prevenzione delle fonti di rischio, Sicurezza dell'hardware, Gestire prontamente gli incidenti di sicurezza e le violazioni dei dati personali.

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

Importante

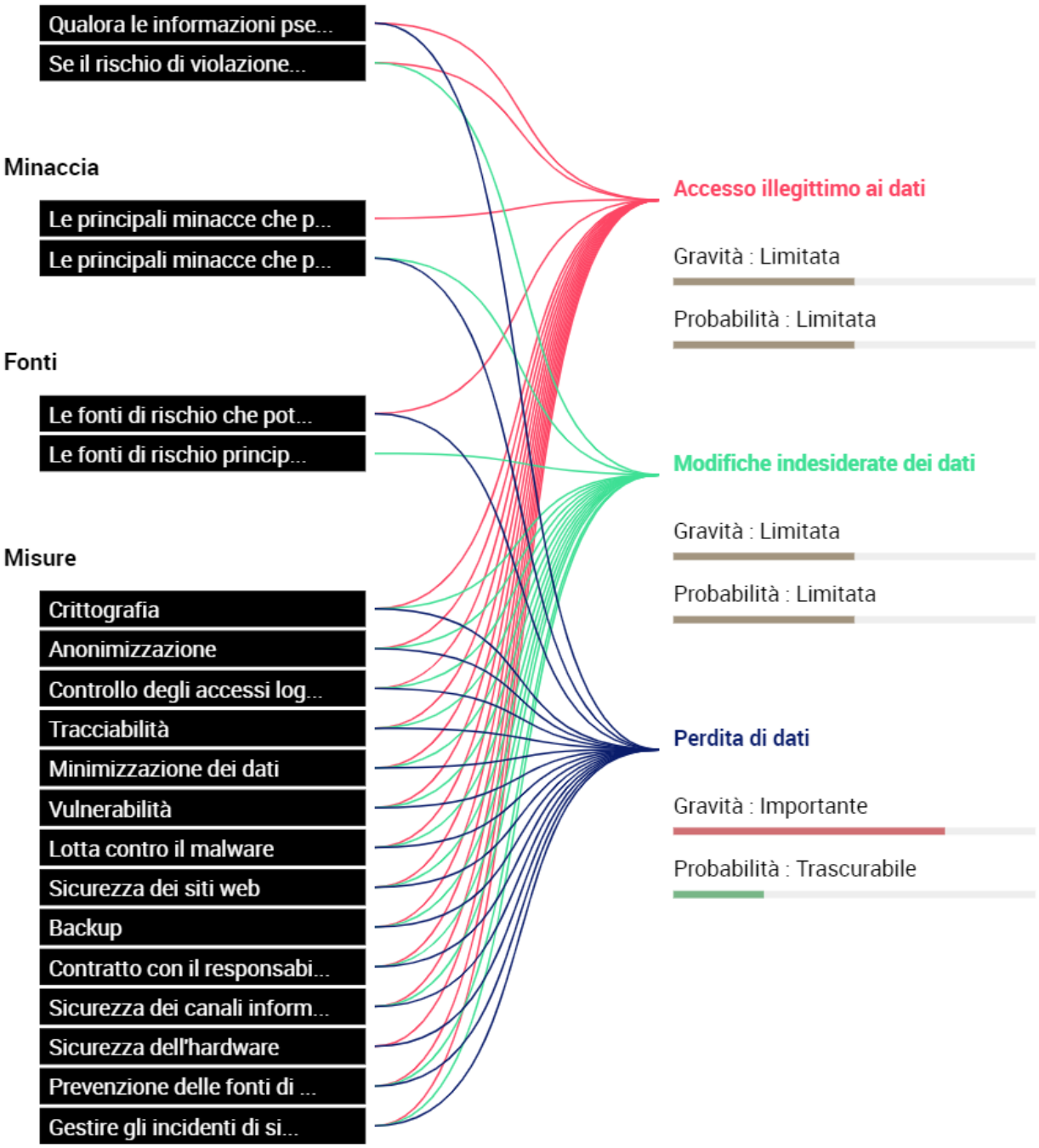
- Anche se i dati sono pseudonimizzati, una perdita di dati potrebbe portare a una violazione della privacy, specialmente se i dati venissero recuperati e utilizzati per scopi non autorizzati o combinati con altre fonti per la re-identificazione.
- Una violazione della privacy può avere conseguenze significative, portando alla divulgazione di informazioni sensibili o sanitarie degli interessati, con possibili danni alla loro reputazione e vita sociale.
- La gravità complessiva di una perdita di dati pseudonimizzati può essere stimata come Moderata-Alta, a seconda delle circostanze. La perdita di dati potrebbe portare a conseguenze significative, specialmente in termini di privacy e reputazione, ma l'implementazione di misure come la crittografia e i backup riduce l'impatto complessivo.

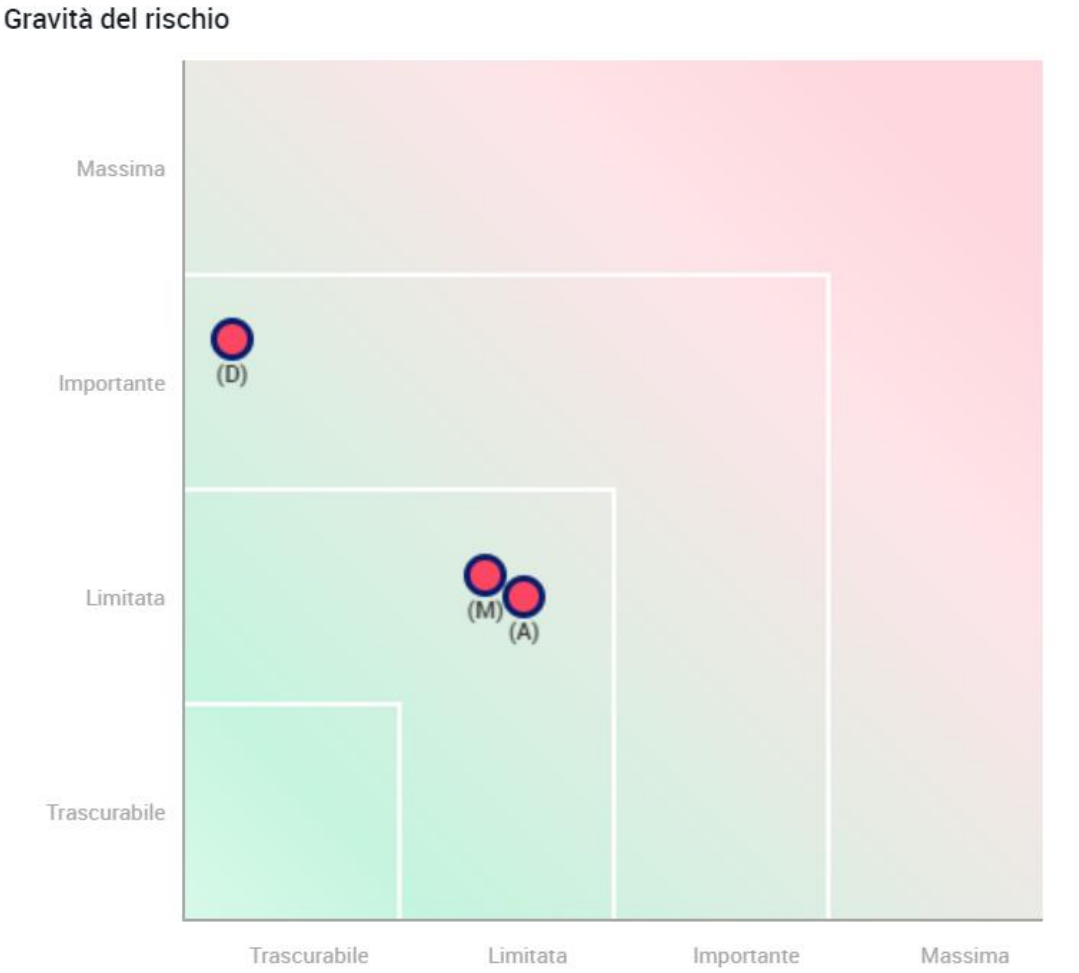
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata

- La probabilità di una perdita di dati nello studio PERICLE può essere stimata come limitata, grazie alle misure di sicurezza implementate, come la crittografia, l'autenticazione multi-fattore, il monitoraggio continuo e i backup regolari. Tuttavia, fattori come l'errore umano o attacchi sofisticati possono ancora rappresentare una minaccia anche se limitata.

Panoramica dei rischi





- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati