IRCCS AOU AL
Santi Antonio e Biagio e Cesare Arrigo
Istituto di Ricovero e Cura a Carattere Scientifico - Azienda Ospedaliero Universitaria di Alessandria

IRCCS Azienda Ospedaliero Universitaria di Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

# Valutazione d’impatto sulla protezione dei dati

# Valutazione d’impatto -SA RIC 05- Sperimentazioni - promotore AOU AL - studio RIGIL

02/11/2026

# Indice

1. Introduzione.....
2. Informazioni essenziali.....
3. Stima del rischio e pre-assessment.....
4. Informazioni sul trattamento.....
5. Valutazione della proporzionalità in relazione alla finalità.....
6. Diritti e principi fondamentali.....
7. Valutazione del rischio.....
    7.1 Misure di sicurezza.....
    7.2 Valutazione del rischio.....
8. Coinvolgimento delle parti interessate.....
9. Note.....

# 1. Introduzione

Il presente documento “Valutazione d’impatto -SA RIC 05- Sperimentazioni - promotore AOU AL - studio RIGIL” ha lo scopo di valutare l’impatto sulla protezione dei dati dell’attività di trattamento “Sperimentazioni - promotore AOU AL”, l’impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati.

# 2. Informazioni essenziali

| | |
|---|---|
| Data di creazione dell’analisi | 22/08/2024 |
| Data generazione documento | 02/11/2026 |
| Data del prossimo controllo | 17/08/2025 |
| Stato | Definitivo |
| Reporter | SILVIA MARIA CERMELLI ; CAROLINA PELAZZA ; ANTONIETTA STARTARI |

# 3. Stima del rischio e pre-assessment

## Pre-Assessment

| Tipologia del trattamento | Risposta |
|---|---|
| Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l’affidabilità o il comportamento, l’ubicazione o gli spostamenti dell’interessato. | No |
| Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi). | No |

IRCCS Azienda Ospedaliero Universitaria di
Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

| | |
|---|---|
| Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc. | No |
| Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 Regolamento UE 2016/679 interconnessi con altri dati personali raccolti per finalità diverse. | No |
| Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). | Sì |
| Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment). | No |
| Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo). | Sì |
| Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 (criteri WP 29). | No |
| Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8). | No |
| Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche. | Sì |

| | |
|---|---|
| Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento. | No |
| Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento. | No |

### Stima del rischio

| Criteri utilizzati per la stima del rischio | Risposta |
|---|---|
| Il trattamento comporta la valutazione o assegnazione di un punteggio inclusiva di profilazione e previsione | No |
| Il trattamento prevede un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente | No |
| Il trattamento consiste in un'attività di monitoraggio sistematico | No |
| Il trattamento coinvolge dati sensibili o dati aventi carattere altamente personale | Sì |
| Il trattamento di dati avviene su larga scala | Sì |
| Il trattamento comporta la creazione di corrispondenze o combinazione di insiemi di dati | No |
| Il trattamento coinvolge categorie di interessati vulnerabili | Sì |
| Il trattamento coinvolge l'uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative | No |
| Il trattamento impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto | No |
| Elevato | |

# 4. Informazioni sul trattamento

| Codice identificativo | Nome | Data di creazione | Data dell'ultima modifica |
|---|---|---|---|
| SA RIC 05 | Sperimentazioni - promotore AOU AL | 22/08/2024 | 02/11/2026 |
| **Descrizione** | | | |
| Attività di ricerca in termini di sperimentazioni e studi clinici con ruolo di promotore di AOU AL che risulta titolare autonomo del trattamento dei dati. Per le sperimentazioni multicentriche AOU AL, in veste di | | | |

| | |
|---|---|
| promotore, ed i centri partecipanti risultano titolari autonomi del trattamento dei dati. | |
| **Finalità del trattamento** | |
| I dati dei soggetti arruolati sono utilizzati per finalità di ricerca scientifica | |
| **Basi giuridiche** | |
| Articolo 6 a) – l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità | |
| Articolo 9 a) – l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche | |
| **Riferimenti normativi** | |
| Regolamento UE 2016/679, Regolamento UE 2018/1725, Regolamento UE 536/2014 (per sperimentazioni interventistiche farmacologiche), Regolamento UE 2023/607 (per sperimentazione su dispositivi medici), DECRETO Ministero della Salute 30 novembre 2021, ICH E6 - R3 Good Clinical Practice, DECRETO LEGISLATIVO 30 giugno 2003, n. 196 e s.m.i | |
| **Origine dei dati** | |
| Raccolti presso l'interessato | |
| **Modalità del trattamento** | |
| Cartaceo | Informatizzato |
| **Categorie di dati** | |
| **Dati personali comuni** | |
| **Comuni** | |
| **Categorie particolari di dati personali** | |
| **Sensibili** | |
| **Categorie di interessati** | |
| Altri soggetti ; Altri soggetti assistiti ; Lavoratori ; Pazienti | |
| **Titolare** | IRCCS Azienda Ospedaliero Universitaria di Alessandria |
| **Responsabile della protezione dei dati** | RPD/DPO ; Silvia Straneo |
| **Diffusione dei dati** | Non viene effettuata la diffusione dei dati. |
| **Trasferimenti e comunicazioni dei dati** | |

| | |
|---|---|
| Non si effettua il trasferimento o la comunicazione dei dati | |
| **Periodo di conservazione dei dati personali** | |
| 20-30 anni | |
| **Applicativi** | Office 365 ; Red Cap - Gestione Dataset osservazionali / Clinical Trials |

## Descrizione sistematica delle componenti del trattamento

Descrizione delle diverse componenti tecnologiche, fisiche ed organizzative che partecipano dell'attività di trattamento valutata.

**Componenti organizzative**

| **Componente** | **Descrizione** |
|---|---|
| Soggetti Interni | **Descrizione sintetica (es. soggetti facenti parte o meno del personale tecnico informatico, descrizione delle attività svolte in relazione ai trattamenti in esame, formazione ricevuta, procedure che ne disciplinano le mansioni, relazioni con altre componenti** |
| | Il personale coinvolto nel trattamento dati, adeguatamente formato come da procedure interne di qualità, svolge le attività previste dal protocollo dello studio clinico di riferimento. |

**Componenti tecnologiche**

| **Componente** | **Descrizione** |
|---|---|
| Applicazioni | **Descrizione sintetica (es. principali caratteristiche, funzionalità, modalità di autenticazione, relazioni con altre componenti)** |
| | Applicativi web/client: - amministrativo contabile per il lavoro amministrativo contabile aziendale e gestione del personale - applicativi sanitari per la gestione del paziente nel suo percorso di cura. Questi applicativi sono certificati come dispositivi medici in classe IIa |
| Infrastrutture IT | **Descrizione sintetica (es. principali caratteristiche tecniche e relazioni con altre componenti)** |

| | |
|---|---|
| | Infrastruttura IT eterogenea: - applicativi con installazione on-premise client (web) server - applicativi con installazione cloud SaaS - previsti sistemi di backup dedicati |
| Rete | **Descrizione sintetica (es. tipologia di rete, tecnologie utilizzate, relazioni con altre componenti)** |
| | Rete LAN dedicata con sistemi di protezione per il perimetro interno basato su Firewall e regole di accesso specifiche per ogni applicativo e per ogni integrazione iter-applicativa. Rete LAN interna segmentata per accesso controllato agli applicativi, alle risorse condivise e alla strumentazione elettromedicale |

# 5. Valutazione della proporzionalità in relazione alla finalità

Tenuto conto che l'attività di trattamento sottoposta a valutazione comporta il trattamento delle categorie di dati personali sopra menzionati, in relazione alle categorie di interessati precedentemente citati, il titolare ritiene che dette categorie di dati siano necessarie e proporzionali al perseguimento della finalità:

I dati dei soggetti arruolati sono utilizzati per finalità di ricerca scientifica

# 6. Diritti e principi fondamentali

## Diritti

| | |
|---|---|
| Accesso | L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso di ottenere l'accesso ai suoi dati personali (Art.15 GDPR 2016/679). Il diritto d'accesso è presente nell'informativa ed è esercitabile attraverso la modulistica presente sul sito aziendale. L'interessato può esercitare i propri diritti rivolgendosi al DPO AOU AL. I dati di contatto del Responsabile della protezione dei dati (DPO) nominato ai sensi dell'art.37 del GDPR sono i seguenti: mail dpo@ospedale.al.it , tel. 0131206710. |

| | |
|---|---|
| Rettifica | L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa (Art. 16 GDPR 2016/679). L'interessato può esercitare i propri diritti rivolgendosi al DPO AOU AL. I dati di contatto del Responsabile della protezione dei dati (DPO) nominato ai sensi dell'art.37 del GDPR sono i seguenti: mail dpo@ospedale.al.it , tel. 0131206710. |
| Cancellazione | L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali. (Art.17 GDPR 2016/679). L'interessato può esercitare i propri diritti rivolgendosi al DPO AOU AL. I dati di contatto del Responsabile della protezione dei dati (DPO) nominato ai sensi dell'art.37 del GDPR sono i seguenti: mail dpo@ospedale.al.it , tel. 0131206710. |
| Portabilità | L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti. (Art 20 GDPR 2016/679). L'interessato può esercitare i propri diritti rivolgendosi al DPO AOU AL. I dati di contatto del Responsabile della protezione dei dati (DPO) nominato ai sensi dell'art.37 del GDPR sono i seguenti: mail dpo@ospedale.al.it , tel. 0131206710. |
| Opposizione | L'articolo 21 del Regolamento generale sulla protezione dei dati (GDPR) disciplina il diritto di opposizione del soggetto interessato. Questo diritto consente al soggetto interessato di opporsi al trattamento dei suoi dati personali in determinate situazioni. Per esercitare il diritto di opposizione, è necessario inviare una richiesta scritta al Titolare del trattamento dei dati. L'interessato può esercitare i propri diritti rivolgendosi al DPO AOU AL. I dati di contatto del Responsabile della protezione dei dati (DPO) nominato ai sensi dell'art.37 del GDPR sono i seguenti: mail dpo@ospedale.al.it , tel. 0131206710. |

| | |
|---|---|
| Limitazione di trattamento | L'articolo 18 del Regolamento Generale sulla Protezione dei Dati (GDPR) disciplina il diritto di limitazione del trattamento dei dati personali. Questo diritto consente alla persona interessata di chiedere al titolare del trattamento di limitare il trattamento dei propri dati personali in determinate circostanze (esattezza dei dati, trattamento illecito, per esercizio o difesa di un diritto in sede giudiziaria…). La limitazione comporta che i dati personali siano segnati e conservati, ma non utilizzati, salvo che per la conservazione degli stessi. L'interessato può esercitare i propri diritti rivolgendosi al DPO AOU AL. I dati di contatto del Responsabile della protezione dei dati (DPO) nominato ai sensi dell'art.37 del GDPR sono i seguenti: mail dpo@ospedale.al.it , tel. 0131206710. |
| Revoca del consenso | L'interessato può altresì ritirare il consenso espresso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca. Per esercitare i sopracitati diritti l'interessato può rivolgersi al Responsabile della protezione dei dati o al Titolare. L'interessato ha il diritto di proporre reclamo a un'autorità di controllo, scrivendo a garante@gpdp.it, oppure protocollo@pec.gpdp.it. (Art 7 GDPR 2016/679). |
| Diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato | In base al Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea, l'art. 22 riconosce il diritto delle persone interessate a non essere soggette a una decisione basata esclusivamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che li riguardano o che li colpisca in modo significativo. Questo diritto mira a preservare la capacità delle persone di essere giudicate da esseri umani e non solo da algoritmi, specialmente in situazioni in cui i risultati possono avere un impatto significativo sulla vita delle persone. |

## Principi

| | |
|---|---|
| I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato | I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le informative sono fornite al paziente in fase di accesso alla struttura e sono disponibili sul sito istituzionale. I dati personali vengono raccolti e trattati per erogare le prestazioni di diagnosi, prevenzione, ricerca e cura. |

| | |
|---|---|
| I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità | I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. Le informative di studio riportano le informazioni dettagliate. |
| I dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali | La Struttura Complessa ICT e innovazione tecnologica con le proprie risorse umane, tecnologiche e strutturali opera costantemente perché tali dati siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali. |

# 7. Valutazione del rischio

Al fine di calcolare la magnitudo di un rischio e si adotta una formula del tipo

$R_1 = f(M, p)$

**IMPATTO (M)**

| | |
|---|---|
| LIEVE | 1 |
| MEDIO | 2 |
| ALTO | 3 |
| ALTISSIMO | 4 |

**X**

**PROBABILITÀ (p)**

| | |
|---|---|
| IMPROBABILE | 1 |
| POCO PROBABILE | 2 |
| PROBABILE | 3 |
| ALTAMENTE PROBABILE | 4 |

**=**

**RISCHIO INIZIALE (R)**

| | |
|---|---|
| BASSO | 1 - 2 |

| | |
|---|---|
| MEDIO | 3 - 4 |
| ALTO | 5 - 8 |
| ALTISSIMO | 9 - 16 |

Dove per:

- **R** si intende il livello di rischio non mitigato;
- **M** si intende l'impatto per i diritti e le libertà degli interessati che viene indicato assegnando un valore da uno a quattro secondo la seguente scala:

| | |
|---|---|
| Lieve | Gli interessati non saranno coinvolti o nella peggiore delle ipotesi potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema. |
| Medio | Gli interessati potrebbero incontrare degli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà |
| Grave | Gli interessati potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di far fronte seppur con gravi difficoltà |
| Gravissimo | Gli interessati potrebbero confrontarsi con conseguenze significative o irreversibili. |

- **p** si intende la probabilità di accadimento del rischio che viene indicata assegnando un valore da uno a quattro secondo la seguente scala:

| | |
|---|---|
| Improbabile | L'avverarsi della minaccia non sembra possibile |
| Poco Probabile | L'avverarsi della minaccia sembra difficile |
| Probabile | L'avverarsi della minaccia sembra possibile |
| Altamente Probabile | L'avverarsi della minaccia sembra probabile |

Un controllo o misura di sicurezza può agire sulla probabilità o l'impatto (o su entrambi) di una minaccia secondo la seguente logica:

$$R_2 = R_1 - \left(M_n\right)$$

dove per:

- $R_2$ si intende il rischio finale, ovverosia il rischio a valle dell'inserimento dei controlli o misure di sicurezza;
- $R_1$ si intende il rischio iniziale come definito più sopra;
- $M_n$ si intende il controllo o la misura di sicurezza.

All'interno del presente passaggio saranno presenti, in ordine

1. l'elenco di misure di sicurezza, suddivise in misure associate in via diretta all'attività di trattamento (misure di sicurezza c.d. "su trattamenti") ed in misure associate ad un asset (misure di sicurezza su "componenti IT", "applicativi" e "luoghi fisici") correlato a propria volta all'attività di trattamento;
2. l'elenco delle minacce comprensivo di: nome assegnato alla minaccia, fonte del rischio (la quale può essere, anche cumulativamente, umana se relativa a soggetti appartenenti all'organizzazione di colui che effettua la valutazione d'impatto, di contesto se relativa a soggetti non appartenenti all'organizzazione del soggetto che effettua la valutazione d'impatto, afferente a strumenti se correlata a malfunzionamenti di strumentazione anche se dipendenti da eventi esterni quali disastri naturali), area di impatto (disponibilità, integrità, riservatezza, anche cumulativamente), valori relativi ad impatto e probabilità (con eventuale motivazione sulle scelte effettuate) e valore specifico del rischio non mitigato;
3. i controlli o misure di sicurezza adottate o valutate nonché la loro incidenza su impatto e probabilità della minaccia.

   https://doc.privacymanager.eu/manuale/valutazione_impatto.html#mitigazione-del-rischio-iniziale-qualitativa
4. Rischio residuo (mitigato).

# 7.1 Misure di sicurezza

## Misure di sicurezza trasversali relative ai trattamenti

| Misura di sicurezza | Stato di adozione e implementazione |
|---|---|

| **Nuove Misure di sicurezza - Da Utilizzare** | |
|---|---|
| MT1 Armadi e contenitori dotati di serrature e/o ignifghi- Conservazione sicura dei documenti cartacei e backup | Applicata |
| MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata |
| MT5 Sistemi di sorveglianza - Misure di controllo accessi ai locali | Applicata |
| MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata |
| MO1 Formazione e sensibilizzazione del personale e istruzioni | Applicata |
| MO3 Definizione puntuale delle regole di archiviazione | Applicata |
| MO4 Definizione del modello organizzativo con assegnazione compiti e responsabilità puntuali e procedure | Applicata |
| MO5 Audit interni ed esterni | Applicata |
| MO7 Misure contratti - Regolamentazione misure applicate nei rapporti con i fornitori | Applicata |
| MO8 Analisi dei rischi | Applicata |
| MV18- Predisposione documento Privacy By design e defalut | Applicata |

## Misure di sicurezza trasversali relative agli asset

| **Misura di sicurezza** | **Stato di adozione e implementazione** |
|---|---|
| **Misure di sicurezza correlate con gli applicativi** | |
| **Nuove Misure di sicurezza - Da Utilizzare** | |
| MT14 Protezione della navigazione web - utilizzo sistemi di web filtering | Applicata |
| MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata |
| MT4 Misure antincendio - Misure di protezione dei bene e dei documenti | Applicata |

| | |
|---|---|
| MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata |
| MT8 Infrastrutture logiche (ex patch di sistema) - utilizzo di sistemi aggiornati | Applicata |
| MV18- Predisposione documento Privacy By design e defalut | Applicata |

## Misure di sicurezza specifiche relative al trattamento

| Categoria | Misura | Stato di adozione e implementazione |
|---|---|---|
| Nuove Misure di sicurezza - Da Utilizzare | M00-Verifica base giuridica e autorizzazionei al trattamento | Applicata |
| | M10- Locali chiusi a chiave o con ingresso controllato | Applicata |
| | MV-2 - Sistema di autenticazione ed autorizzazione | Applicata |
| | MV-6 - Tracciabilità accessi risorse | Applicata |
| | MV-10 - Cifratura del dato | Applicata |
| | MV-12 - Pseudonimizzazione | Applicata |
| | MV-17 - Protezione applicativa (WAF WEB application firewall) | Applicata |

## 7.2 Valutazione del rischio

| Minaccia | Categoria | Aree di impatto | Fonti di rischio |
|---|---|---|---|
| Divulgazione accidentale di informazioni | Minacce SMART - BASE | Riservatezza | Umano |
| **Descrizione** | | | |
| **Anche da parte dei dipendenti** | | | |
| **Elemento** | | **Valore iniziale numerico** | **Valore iniziale** |
| Impatto | | 3 | Grave |
| Probabilità | | 2 | Poco probabile |
| **Livello di rischio iniziale** | | 6 | Alto |
| **Misure di sicurezza** | | | |
| **Categoria** | **Misura** | **Mitigazione Impatto** | **Mitigazione probabilità** |
| Nuove Misure di sicurezza - Da Utilizzare | MT1 Armadi e contenitori dotati di serrature e/o ignifghi- Conservazione sicura dei documenti cartacei e backup | Applicata | Applicata |
| | MT14 Protezione della navigazione web - utilizzo sistemi di web filtering | Applicata | Applicata |
| | MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata | Applicata |
| | MT4 Misure antincendio - Misure di protezione dei bene e dei documenti | Applicata | Applicata |

| | | | |
|---|---|---|---|
| | MT5 Sistemi di sorveglianza - Misure di controllo accessi ai locali | Applicata | Applicata |
| | MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata | Applicata |
| | MT8 Infrastrutture logiche (ex patch di sistema) - utilizzo di sistemi aggiornati | Applicata | Applicata |
| | M00-Verifica base giuridica e autorizzazionei al trattamento | Applicata | Applicata |
| | MO1 Formazione e sensibilizzazione del personale e istruzioni | Applicata | Applicata |
| | MO3 Definizione puntuale delle regole di archiviazione | Applicata | Applicata |
| | MO4 Definizione del modello organizzativo con assegnazione compiti e responsabilità puntuali e procedure | Applicata | Applicata |
| | MO5 Audit interni ed esterni | Applicata | Applicata |
| | MO7 Misure contratti - Regolamentazione misure applicate nei rapporti con i fornitori | Applicata | Applicata |

| | | | |
|---|---|---|---|
| | M10- Locali chiusi a chiave o con ingresso controllato | Applicata | Applicata |
| | MO8 Analisi dei rischi | Applicata | Applicata |
| | MV-2 - Sistema di autenticazione ed autorizzazione | Applicata | Applicata |
| | MV-6 - Tracciabilità accessi risorse | Applicata | Applicata |
| | MV-10 - Cifratura del dato | Applicata | Applicata |
| | MV-12 - Pseudonimizzazione | Applicata | Applicata |
| | MV-17 - Protezione applicativa (WAF WEB application firewall) | Applicata | Applicata |
| | MV18- Predisposione documento Privacy By design e defalut | Applicata | Applicata |
| **Elemento** | | **Valore finale numerico** | **Valore finale** |
| Impatto | | 1 | Lieve |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio finale** | | 1 | Basso |
| **Mitigazione totale d'impatto** | | **Mitigazione totale di probabilità** | |
| Totale | | Totale | |

| Minaccia | Categoria | Aree di impatto | Fonti di rischio |
|---|---|---|---|
| Accesso illegittimo ai dati | Minacce SMART - BASE | Riservatezza | Umano ; Contesto ; Strumenti |
| **Elemento** | | **Valore iniziale numerico** | **Valore iniziale** |
| Impatto | | 3 | Grave |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio iniziale** | | 3 | Medio |
| **Misure di sicurezza** | | | |
| **Categoria** | **Misura** | **Mitigazione Impatto** | **Mitigazione probabilità** |
| Nuove Misure di sicurezza - Da Utilizzare | MT1 Armadi e contenitori dotati di serrature e/o ignifghi- Conservazione sicura dei documenti cartacei e backup | Applicata | Applicata |
| | MT14 Protezione della navigazione web - utilizzo sistemi di web filtering | Applicata | Applicata |
| | MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata | Applicata |
| | MT4 Misure antincendio - Misure di protezione dei bene e dei documenti | Applicata | Applicata |
| | MT5 Sistemi di sorveglianza - Misure di controllo accessi ai locali | Applicata | Applicata |

IRCCS Azienda Ospedaliero Universitaria di Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

| | | | |
|---|---|---|---|
| | MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata | Applicata |
| | MT8 Infrastrutture logiche (ex patch di sistema) - utilizzo di sistemi aggiornati | Applicata | Applicata |
| | M00-Verifica base giuridica e autorizzazionei al trattamento | Applicata | Applicata |
| | MO1 Formazione e sensibilizzazione del personale e istruzioni | Applicata | Applicata |
| | MO3 Definizione puntuale delle regole di archiviazione | Applicata | Applicata |
| | MO4 Definizione del modello organizzativo con assegnazione compiti e responsabilità puntuali e procedure | Applicata | Applicata |
| | MO5 Audit interni ed esterni | Applicata | Applicata |
| | MO7 Misure contratti - Regolamentazione misure applicate nei rapporti con i fornitori | Applicata | Applicata |
| | M10- Locali chiusi a chiave o con ingresso controllato | Applicata | Applicata |

| | | | |
|---|---|---|---|
| | MO8 Analisi dei rischi | Applicata | Applicata |
| | MV-2 - Sistema di autenticazione ed autorizzazione | Applicata | Applicata |
| | MV-6 - Tracciabilità accessi risorse | Applicata | Applicata |
| | MV-10 - Cifratura del dato | Applicata | Applicata |
| | MV-12 - Pseudonimizzazione | Applicata | Applicata |
| | MV-17 - Protezione applicativa (WAF WEB application firewall) | Applicata | Applicata |
| | MV18- Predisposione documento Privacy By design e defalut | Applicata | Applicata |
| **Elemento** | | **Valore finale numerico** | **Valore finale** |
| Impatto | | 1 | Lieve |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio finale** | | 1 | Basso |
| **Mitigazione totale d'impatto** | | **Mitigazione totale di probabilità** | |
| Totale | | Totale | |

| Minaccia | Categoria | Aree di impatto | Fonti di rischio |
|---|---|---|---|
| Modifiche indesiderate dei dati | Minacce SMART - BASE | Integrità | Umano ; Contesto ; Strumenti |
| **Elemento** | | **Valore iniziale numerico** | **Valore iniziale** |
| Impatto | | 4 | Gravissimo |
| Probabilità | | 2 | Poco probabile |
| **Livello di rischio iniziale** | | 8 | Alto |
| **Misure di sicurezza** | | | |
| **Categoria** | **Misura** | **Mitigazione Impatto** | **Mitigazione probabilità** |
| Nuove Misure di sicurezza - Da Utilizzare | MT1 Armadi e contenitori dotati di serrature e/o ignifghi- Conservazione sicura dei documenti cartacei e backup | Applicata | Applicata |
| | MT14 Protezione della navigazione web - utilizzo sistemi di web filtering | Applicata | Applicata |
| | MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata | Applicata |
| | MT4 Misure antincendio - Misure di protezione dei bene e dei documenti | Applicata | Applicata |
| | MT5 Sistemi di sorveglianza - Misure di controllo accessi ai locali | Applicata | Applicata |

IRCCS Azienda Ospedaliero Universitaria di Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

| | | | |
|---|---|---|---|
| | MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata | Applicata |
| | MT8 Infrastrutture logiche (ex patch di sistema) - utilizzo di sistemi aggiornati | Applicata | Applicata |
| | M00-Verifica base giuridica e autorizzazionei al trattamento | Applicata | Applicata |
| | MO1 Formazione e sensibilizzazione del personale e istruzioni | Applicata | Applicata |
| | MO3 Definizione puntuale delle regole di archiviazione | Applicata | Applicata |
| | MO4 Definizione del modello organizzativo con assegnazione compiti e responsabilità puntuali e procedure | Applicata | Applicata |
| | MO5 Audit interni ed esterni | Applicata | Applicata |
| | MO7 Misure contratti - Regolamentazione misure applicate nei rapporti con i fornitori | Applicata | Applicata |
| | M10- Locali chiusi a chiave o con ingresso controllato | Applicata | Applicata |

| | | | |
|---|---|---|---|
| | MO8 Analisi dei rischi | Applicata | Applicata |
| | MV-2 - Sistema di autenticazione ed autorizzazione | Applicata | Applicata |
| | MV-6 - Tracciabilità accessi risorse | Applicata | Applicata |
| | MV-10 - Cifratura del dato | Applicata | Applicata |
| | MV-12 - Pseudonimizzazione | Applicata | Applicata |
| | MV-17 - Protezione applicativa (WAF WEB application firewall) | Applicata | Applicata |
| | MV18- Predisposione documento Privacy By design e defalut | Applicata | Applicata |
| **Elemento** | | **Valore finale numerico** | **Valore finale** |
| Impatto | | 1 | Lieve |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio finale** | | 1 | Basso |
| **Mitigazione totale d'impatto** | | **Mitigazione totale di probabilità** | |
| Totale | | Totale | |

| Minaccia | Categoria | Aree di impatto | Fonti di rischio |
|---|---|---|---|
| Perdita di dati | Minacce SMART - BASE | Disponibilità | Umano ; Contesto ; Strumenti |
| **Elemento** | | **Valore iniziale numerico** | **Valore iniziale** |
| Impatto | | 3 | Grave |
| Probabilità | | 2 | Poco probabile |
| **Livello di rischio iniziale** | | 6 | Alto |
| **Misure di sicurezza** | | | |
| **Categoria** | **Misura** | **Mitigazione Impatto** | **Mitigazione probabilità** |
| Nuove Misure di sicurezza - Da Utilizzare | MT1 Armadi e contenitori dotati di serrature e/o ignifghi- Conservazione sicura dei documenti cartacei e backup | Applicata | Applicata |
| | MT14 Protezione della navigazione web - utilizzo sistemi di web filtering | Applicata | Applicata |
| | MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata | Applicata |
| | MT4 Misure antincendio - Misure di protezione dei bene e dei documenti | Applicata | Applicata |
| | MT5 Sistemi di sorveglianza - Misure di controllo accessi ai locali | Applicata | Applicata |

IRCCS Azienda Ospedaliero Universitaria di Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

| | | | |
|---|---|---|---|
| | MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata | Applicata |
| | MT8 Infrastrutture logiche (ex patch di sistema) - utilizzo di sistemi aggiornati | Applicata | Applicata |
| | M00-Verifica base giuridica e autorizzazionei al trattamento | Applicata | Applicata |
| | MO1 Formazione e sensibilizzazione del personale e istruzioni | Applicata | Applicata |
| | MO3 Definizione puntuale delle regole di archiviazione | Applicata | Applicata |
| | MO4 Definizione del modello organizzativo con assegnazione compiti e responsabilità puntuali e procedure | Applicata | Applicata |
| | MO5 Audit interni ed esterni | Applicata | Applicata |
| | MO7 Misure contratti - Regolamentazione misure applicate nei rapporti con i fornitori | Applicata | Applicata |
| | M10- Locali chiusi a chiave o con ingresso controllato | Applicata | Applicata |

| | | | |
|---|---|---|---|
| | MO8 Analisi dei rischi | Applicata | Applicata |
| | MV-2 - Sistema di autenticazione ed autorizzazione | Applicata | Applicata |
| | MV-6 - Tracciabilità accessi risorse | Applicata | Applicata |
| | MV-10 - Cifratura del dato | Applicata | Applicata |
| | MV-12 - Pseudonimizzazione | Applicata | Applicata |
| | MV-17 - Protezione applicativa (WAF WEB application firewall) | Applicata | Applicata |
| | MV18- Predisposione documento Privacy By design e defalut | Applicata | Applicata |
| **Elemento** | | **Valore finale numerico** | **Valore finale** |
| Impatto | | 1 | Lieve |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio finale** | | 1 | Basso |
| **Mitigazione totale d'impatto** | | **Mitigazione totale di probabilità** | |
| Totale | | Totale | |

| Minaccia | Categoria | Aree di impatto | Fonti di rischio |
|---|---|---|---|
| Furto d'identità | Minacce SMART - BASE | Disponibilità ; Riservatezza ; Integrità | Umano ; Contesto ; Strumenti |
| **Elemento** | | **Valore iniziale numerico** | **Valore iniziale** |
| Impatto | | 2 | Medio |
| Probabilità | | 2 | Poco probabile |
| **Livello di rischio iniziale** | | 4 | Medio |
| **Misure di sicurezza** | | | |
| **Categoria** | **Misura** | **Mitigazione Impatto** | **Mitigazione probabilità** |
| Nuove Misure di sicurezza - Da Utilizzare | MT1 Armadi e contenitori dotati di serrature e/o ignifghi- Conservazione sicura dei documenti cartacei e backup | Applicata | Applicata |
| | MT14 Protezione della navigazione web - utilizzo sistemi di web filtering | Applicata | Applicata |
| | MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata | Applicata |
| | MT4 Misure antincendio - Misure di protezione dei bene e dei documenti | Applicata | Applicata |
| | MT5 Sistemi di sorveglianza - Misure di controllo accessi ai locali | Applicata | Applicata |

IRCCS Azienda Ospedaliero Universitaria di Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

| | | | |
|---|---|---|---|
| | MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata | Applicata |
| | MT8 Infrastrutture logiche (ex patch di sistema) - utilizzo di sistemi aggiornati | Applicata | Applicata |
| | M00-Verifica base giuridica e autorizzazionei al trattamento | Applicata | Applicata |
| | MO1 Formazione e sensibilizzazione del personale e istruzioni | Applicata | Applicata |
| | MO3 Definizione puntuale delle regole di archiviazione | Applicata | Applicata |
| | MO4 Definizione del modello organizzativo con assegnazione compiti e responsabilità puntuali e procedure | Applicata | Applicata |
| | MO5 Audit interni ed esterni | Applicata | Applicata |
| | MO7 Misure contratti - Regolamentazione misure applicate nei rapporti con i fornitori | Applicata | Applicata |
| | M10- Locali chiusi a chiave o con ingresso controllato | Applicata | Applicata |

| | | | |
|---|---|---|---|
| | MO8 Analisi dei rischi | Applicata | Applicata |
| | MV-2 - Sistema di autenticazione ed autorizzazione | Applicata | Applicata |
| | MV-6 - Tracciabilità accessi risorse | Applicata | Applicata |
| | MV-10 - Cifratura del dato | Applicata | Applicata |
| | MV-12 - Pseudonimizzazione | Applicata | Applicata |
| | MV-17 - Protezione applicativa (WAF WEB application firewall) | Applicata | Applicata |
| | MV18- Predisposione documento Privacy By design e defalut | Applicata | Applicata |
| **Elemento** | | **Valore finale numerico** | **Valore finale** |
| Impatto | | 1 | Lieve |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio finale** | | 1 | Basso |
| **Mitigazione totale d'impatto** | | **Mitigazione totale di probabilità** | |
| Totale | | Totale | |

| Minaccia | Categoria | Aree di impatto | Fonti di rischio |
|---|---|---|---|
| Trattamento illecito | Minacce SMART - BASE | Disponibilità ; Riservatezza ; Integrità | Umano ; Contesto ; Strumenti |
| **Elemento** | | **Valore iniziale numerico** | **Valore iniziale** |
| Impatto | | 2 | Medio |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio iniziale** | | 2 | Basso |
| **Misure di sicurezza** | | | |
| **Categoria** | **Misura** | **Mitigazione Impatto** | **Mitigazione probabilità** |
| Nuove Misure di sicurezza - Da Utilizzare | MT1 Armadi e contenitori dotati di serrature e/o ignifghi- Conservazione sicura dei documenti cartacei e backup | Applicata | Applicata |
| | MT14 Protezione della navigazione web - utilizzo sistemi di web filtering | Applicata | Applicata |
| | MT19 Backup e restore - Politiche e mezzi implementati per eseguire il backup e il restore, test periodico dei backup | Applicata | Applicata |
| | MT4 Misure antincendio - Misure di protezione dei bene e dei documenti | Applicata | Applicata |
| | MT5 Sistemi di sorveglianza - Misure di controllo accessi ai locali | Applicata | Applicata |

IRCCS Azienda Ospedaliero Universitaria di Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

| | | | |
|---|---|---|---|
| | MT6 Gestione delle postazioni di lavoro - Misure adottate per ridurre la possibilità che le postazioni di lavoro vengano sfruttate per violare la sicurezza dei dati personali | Applicata | Applicata |
| | MT8 Infrastrutture logiche (ex patch di sistema) - utilizzo di sistemi aggiornati | Applicata | Applicata |
| | M00-Verifica base giuridica e autorizzazionei al trattamento | Applicata | Applicata |
| | MO1 Formazione e sensibilizzazione del personale e istruzioni | Applicata | Applicata |
| | MO3 Definizione puntuale delle regole di archiviazione | Applicata | Applicata |
| | MO4 Definizione del modello organizzativo con assegnazione compiti e responsabilità puntuali e procedure | Applicata | Applicata |
| | MO5 Audit interni ed esterni | Applicata | Applicata |
| | MO7 Misure contratti - Regolamentazione misure applicate nei rapporti con i fornitori | Applicata | Applicata |
| | M10- Locali chiusi a chiave o con ingresso controllato | Applicata | Applicata |

| | | | |
|---|---|---|---|
| | MO8 Analisi dei rischi | Applicata | Applicata |
| | MV-2 - Sistema di autenticazione ed autorizzazione | Applicata | Applicata |
| | MV-6 - Tracciabilità accessi risorse | Applicata | Applicata |
| | MV-10 - Cifratura del dato | Applicata | Applicata |
| | MV-12 - Pseudonimizzazione | Applicata | Applicata |
| | MV-17 - Protezione applicativa (WAF WEB application firewall) | Applicata | Applicata |
| | MV18- Predisposione documento Privacy By design e defalut | Applicata | Applicata |
| **Elemento** | | **Valore finale numerico** | **Valore finale** |
| Impatto | | 1 | Lieve |
| Probabilità | | 1 | Improbabile |
| **Livello di rischio finale** | | 1 | Basso |
| **Mitigazione totale d'impatto** | | **Mitigazione totale di probabilità** | |
| Totale | | Totale | |

## Riassunto ed esito dell'analisi del rischio

| Minaccia | Rischio iniziale | Rischio residuo |
|---|---|---|
| Divulgazione accidentale di informazioni | 6 | 1 |
| Accesso illegittimo ai dati | 3 | 1 |
| Modifiche indesiderate dei dati | 8 | 1 |
| Perdita di dati | 6 | 1 |
| Furto d'identità | 4 | 1 |
| Trattamento illecito | 2 | 1 |

## Livello di rischio complessivo per area

| Area di impatto | Livello di rischio |
|---|---|
| Riservatezza | Basso |
| Integrità | Basso |
| Disponibilità | Basso |

## Livello di rischio complessivo iniziale

## Livello di rischio complessivo residuo

Basso

# 8. Coinvolgimento delle parti interessate

| Domanda | Risposta |
|---|---|
| **Sono state raccolte le opinioni degli interessati o dei loro rappresentanti?** | No |
| **È stato coinvolto il Responsabile della Protezione dei Dati?** | Sì |
| Il DPO è stato coinvolto in fase di redazione del trattamento e di relativa DPIA. | |

# 9. Note

Titolo e acronimo: Valutazione dell'esposizione a sostanze perfluoroalchiliche (PFAS) di soggetti residenti in un raggio di 3 e 6 chilometri dal Polo Chimico di Spinetta Marengo e sul resto del territorio del comune di Alessandria (RIGIL)

Promotore: Dipartimento di Scienze e Innovazione Tecnologica, Università del Piemonte Orientale, Viale Michel, 11, 15121 Alessandria - Dipartimento Attività Integrate Ricerca e Innovazione, Azienda Ospedaliera Nazionale SS Antonio e Biagio e Cesare Arrigo, Via Venezia n. 16, 15121 Alessandria

Sperimentatore Principale: Dr Bertolotti Marinella, SC Infrastruttura Ricerca Formazione Innovazione, Dipartimento Attività Integrate Ricerca e Innovazione

Tipologia dello studio: osservazionale pilota prospettico, monocentrico, no-profit

Breve descrizione e obiettivo: I PFAS (sostanze perfluoroalchiliche) sono composti chimici altamente resistenti alla degradazione, utilizzati in molte applicazioni industriali e civili per le loro proprietà idrofobiche e termoresistenti, ma considerati inquinanti ambientali persistenti e potenzialmente pericolosi per la salute umana. Queste sostanze, grazie alla loro struttura chimica stabile e alla natura anfifilica, si diffondono facilmente nell'ambiente e possono accumularsi negli organismi viventi, compreso l'uomo, entrando nella catena alimentare. Sono stati riscontrati effetti tossici a livello epatico, endocrino, metabolico ed epigenetico. A Spinetta Marengo, vicino ad Alessandria, dove è attivo un polo chimico produttore di fluoroderivati, è stato riscontrato un significativo inquinamento da PFAS, con livelli elevati rilevati nel sangue dei residenti. Per questo sono stati avviati studi di biomonitoraggio per valutare l'esposizione e gli effetti sulla salute della popolazione locale, mediante analisi di campioni biologici e ambientali, con l'obiettivo di individuare eventuali associazioni tra la presenza di PFAS e alterazioni biologiche nei soggetti esposti. Questo studio vuole valutare quantitativamente e qualitativamente l'esposizione a PFAS di soggetti residenti nel comune di Alessandria in un raggio di 3 e 6 chilometri dal polo chimico di Spinetta Marengo e nel resto del territorio comunale

IRCCS Azienda Ospedaliero Universitaria di
Alessandria
15121
Via Venezia, 16
Alessandria

C.F.- P.IVA 01640560064

t. 0131.206111
F.
W. https://www.ospedale.al.it/
info@ospedale.al.it

Popolazione in studio: Il campione in studio sarà costituito da 300 soggetti totali: sarà reclutato un campione casuale, stratificato per genere ed età, proporzionale ai residenti di ciascuna delle seguenti aree:
• 100 residenti entro un raggio di 3 km dal Polo Chimico di Spinetta Marengo;
• 100 residenti entro un raggio compreso tra i 3 km ed i 6 km dal Polo Chimico di Spinetta Marengo;
• 100 residenti a partire da un raggio di 6 km dal Polo Chimico di Spinetta Marengo sino a comprendere l'intero territorio del comune di Alessandria.

Le fasce di età considerate sono le seguenti:
• 65 anni.

Il Titolare del trattamento

IRCCS Azienda Ospedaliero Universitaria di Alessandria