Versione 2.0
Data 18/07/2024

DATA PROTECTION IMPACT ASSESSMENT

Autori documento	Dr. Pasquale Palladino Dr.ssa Elena Zanzottera Ferrari THIN Srl Piazza Vetra, 17 - 20123 Milano
Validatore	Avv Marco Maglio, Responsabile della protezione di dati di THIN Srl

SOMMARIO

1. CONTESTO

1.1.Panoramica del trattamento

Quale è il trattamento in considerazione?

The Health Improvement Network (THIN®) è un osservatorio epidemiologico (di seguito anche "Osservatorio THIN") finalizzato alla creazione di una raccolta dati europea di dati clinici anonimizzati, alimentato dai Medici di Medicina Generale (MMG) partecipanti all'Osservatorio THIN (di seguito "Medici Ricercatori"). THIN® permette una lettura di dati che prevedono l'osservazione di differenti variabili, ciascuna in una serie di periodi di tempo (cosiddetta lettura longitudinale dei dati), fornendo informazioni e indicatori essenziali per la ricerca medica. I dati presenti in THIN® sono opportunamente trattati in modo da eliminare gli identificatori personali dei pazienti e anonimizzarli, e comprendono sintomi, diagnosi, risultati di test e trattamenti sanitari. Questi indicatori, generati nell'ambito del rapporto tra il medico ed il paziente, vengono utilizzati per diversi scopi: ricerca medica, valutazione dell'efficacia terapeutica, miglioramento dell'assistenza ai pazienti, riduzione dei ritardi nelle cure, ecc.

THIN® è costituito da file generati dall'estrattore installato presso la postazione del Medico Ricercatore. I dati sono trasferiti a THIN Srl solo dopo che il Medico Ricercatore fornisce ai pazienti che entrano in contatto con lui, un'informativa che descrive la finalità della ricerca svolta da THIN Srl, i come titolare del trattamento e dopo aver raccolto il consenso degli stessi. Una informativa breve viene inoltre esposta in tutti gli ambulatori dei Medici Ricercatori partecipanti al network THIN®, mentre l'informativa estesa é resa disponibile al paziente prima di raccogliere il suo consenso. Se a seguito di ciò il paziente esprime il suo consenso all'utilizzo dei suoi dati clinici per finalità di ricerca e di successiva anonimizzazione, il Medico Ricercatore avvia il trattamento dei dati riferiti al paziente in oggetto tramite l'estrattore installato presso la sua postazione.
Per quanto riguarda invece i pazienti deceduti o non contattabili i dati potranno essere raccolti utilizzando le modalità previste dall'articolo 110, comma 1, secondo capoverso del Codice in materia di protezione dei dati personali così come modificato dalla legge 29 aprile 2024, n. 56.

Il processo di anonimizzazione progettato per implementare e realizzare l'Osservatorio THIN si articola oggi in tre "step di lavorazione" che, partendo dai dati personali raccolti presso il Medico Ricercatore, vede l'applicazione di algoritmi e tecniche di de-identificazione, nonché la presenza di contratti tra i diversi soggetti che vietano di porre essere atti di re-identificazione.

Quali sono i ruoli attribuiti nel trattamento?

- **Titolare del trattamento dei dati**

  THIN Srl, con sede a Milano (Italia), in Piazza Vetra, 17 (nel testo identificata anche come "Titolare")

- **Responsabili del trattamento per il processo di de-identificazione e di anonimizzazione**

  Medici di Medicina Generale che aderiscono all'Osservartorio THIN, responsabili del trattamento contrattualizzati da THIN Srl (nel testo identificati anche come "Medici Ricercatori").

  Mediatec Informatica Srl, con sede a Loreo (Italia), Calle Costa 14, società che produce e commercializza il software di gestione ambulatoriale Medico 2000, (di seguito "Mediatec"), responsabile del trattamento contrattualizzata da THIN Srl.

  Edgewhere SAS, con sede a Parigi (Francia), 24 rue de Maubeuge, società che fornisce servizi di rafforzamento delle tecniche di de-identificazione dei dati (di seguito "Edgewhere") subresponsabile del trattamento contrattualizzato da Mediatec Informatica Srl.

  Cegedim.cloud SASU, con sede a Boulogne-Billancourt (Francia), 137 rue d'Aguesseau, società che fornisce le infrastrutture tecniche di hosting e la manutenzione delle stesse (comprese le postazioni di lavoro), fornitore di hosting di dati sanitari (HDS) (di seguito "Cegedim.cloud"), responsabile del trattamento contrattualizzata da THIN Srl.

Ci sono standard applicabili al trattamento?

Le fonti normative, regolamentari e gli standard applicabili al trattamento sono:

- le certificazioni per hosting e infrastrutture tenendo conto di Certificazione ISO 27001

- Piano di controllo ISAE 3402

Certificazione come host di dati sanitari (HDS) rilasciata dalla HAS (Haute Autorité de Santé)

· ISO/IEC 27001:2013.

· D.Lgs. 30 giugno 2003 n. 196 e s.m.i., Codice in materia di protezione dei dati personali;

· Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

· Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n.10" approvate dal Garante per la protezione dei dati personali il 19 dicembre del 2018;

· Provvedimento "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice" adottato dal Garante per la protezione dei dati

personali il 9 giugno 2024.

1.2. **Dati, processi e risorse di supporto** ***(OMISSIS, informazioni riservate)***

2. PRINCIPI FONDAMENTALI (*OMISSIS, informazioni riservate)*

2.1. **Proporzionalità e necessità** ***(OMISSIS, informazioni riservate)***
2.2. **Misure a tutela dei diritti degli interessati (*OMISSIS, informazioni riservate)***

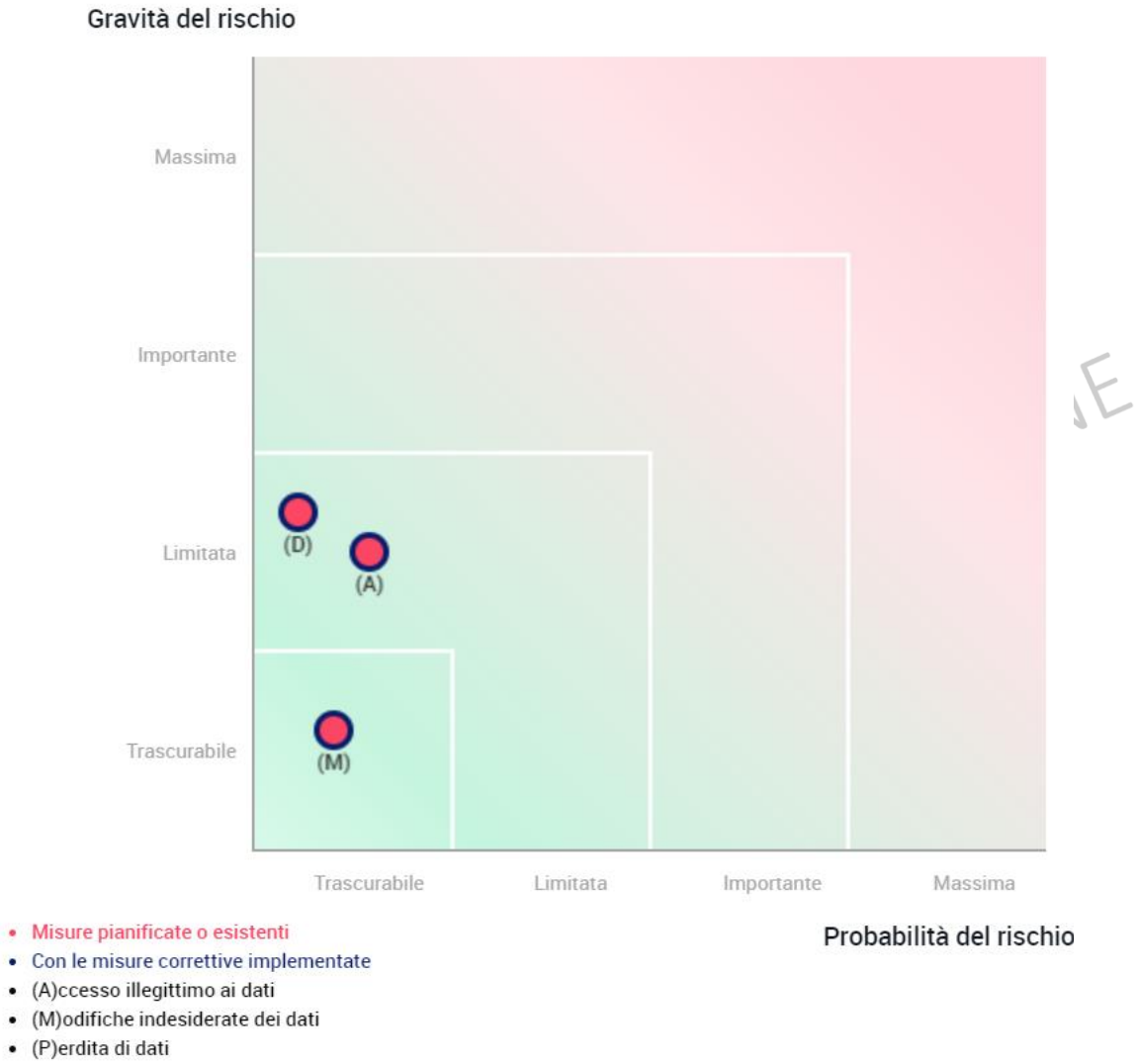
3. RISCHI (OMISSIS, informazioni riservate)

3.1. Misure di de-identificazione e successiva anonimizzazione (*OMISSIS, informazioni riservate)*

3.2. Altre misure di sicurezza tecniche esistenti (*OMISSIS, informazioni riservate)*
3.3. Altre misure di sicurezza organizzative esistenti *(OMISSIS, informazioni riservate)*
3.4. Accesso illegittimo ai dati (*OMISSIS, informazioni riservate)*
3.5. Modifiche indesiderate dei dati (*OMISSIS, informazioni riservate)*
3.6. Perdita di dati *(OMISSIS, informazioni riservate)*

4. CONVALIDA

4.1. Mappatura del rischio



4.2. Piano d'azione

Saranno implementati dei controlli con cadenza minima annuale per verificare che la probabilità e la gravità del rischio nel caso di accesso illegittimo ai dati, di modifiche indesiderate dei dati e di perdita dei dati rimangano nei range identificati nella presente DPIA. Tali analisi saranno prodotte entro la fine del mese di marzo di ogni anno solare con i dati disponibili alla chiusura dell'anno precedente.

4.3. Parere del DPO

Esaminata la descrizione del trattamento il Responsabile della protezione dei dati ritiene che i rischi connessi all'uso improprio dei dati trattati siano adeguatamente gestiti. Il trattamento di dati personali svolto da THIN Srl finalizzato all'utilizzo dei dati in relazione alla attività di ricerca descritta in questa valutazione di impatto del trattamento dei dati personali é strutturato nel rispetto dei principi di privacy by design e privacy by default previsti dall'art. 25 del Regolamento UE 2016/679 e dei principi previsti dall'art. 5 del medesimo Regolamento. Le misure di sicurezza sono adeguate e tengono conto dei ruoli del trattamento assunti alle parti (in particolare da THIN Srl come titolare del trattamento in quanto soggetto che promuove l'attività di ricerca prevista dall'Osservatorio THIN) e della natura dei dati personali trattati (che riguardano dati riferiti a categorie particolari).

Parere formulato il 23/07/2024

5. ALLEGATI

5.1. Allegato A**:** Assessment Bl4ckSwan **Srl**