AZIENDA SANITARIA LOCALE DI PESCARA

Sede Legale:
Via Renato Paolini, 45
65124 Pescara
P. IVA 01397530682

IL DIRETTORE GENERALE

Pescara,

A tutti i Direttori/Dirigenti Responsabili UOC/UOSD, in qualità di Soggetti Autorizzati al Trattamento dei dati Personali con Delega (SATD)
p.c.
Ill.mo Direttore Sanitario
Ill.mo Direttore UOC Sistemi Informativi
Spett.le Ufficio Privacy e Sicurezza delle Informazioni

Oggetto: **Richiesta di pseudonimizzazione e o cifratura dei dati: prescrizioni a carico dei dipendenti della ASL di Pescara, nominati in qualità di SATD e di SAT.**

Per **dato personale** si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (l'interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (articolo 4, punto 1), del Regolamento UE 2016/679, di seguito, "GDPR").

Per **pseudonimizzazione** si intende il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile (articolo 4, punto 5), del GDPR).

La pseudonimizzazione svolge un ruolo importante nel GDPR come misura di sicurezza (articolo 32 del GDPR), così come nell'ambito della protezione dei dati (articolo 25 del GDPR). Il vantaggio più evidente legato alla pseudonimizzazione consiste nell'occultare l'identità degli interessati a terzi (diversi da chi effettua la pseudonimizzazione) nell'ambito di una specifica operazione di trattamento dei dati. La pseudonimizzazione, tuttavia, non si limita a occultare la reale identità, ma concorre all'obiettivo di proteggere i dati anche grazie all'inassociabilità, ossia riducendo il rischio che i dati relativi alla privacy vengano collegati tra differenti domini di trattamento dei dati.

Inoltre, la pseudonimizzazione (essendo una tecnica di minimizzazione dei dati) può contribuire al principio della minimizzazione dei dati ai sensi del GDPR, come nel caso in cui il titolare del trattamento non debba avere accesso all'identità reale degli interessati, ma solo ai loro pseudonimi. Infine, un altro importante vantaggio connesso alla pseudonimizzazione, da non sottovalutare, è costituito dall'accuratezza dei dati.

Nell'ambito di ciascuna operazione di trattamento dei dati personali, il Soggetto Autorizzato al Trattamento dei dati Personali con Delega (SATD) dovrà fare in modo che i dati personali, **trasmessi a soggetti terzi** (altra ASL, Regione Abruzzo, Università, Enti locali, Autorità di Pubblica Sicurezza, Associazioni, ecc.) rispettino i seguenti principi:

a. adozione di misure tecniche e organizzative adeguate, in linea con il rispetto dei **principi di liceità, correttezza e trasparenza**;
b. raccolti per finalità determinate, esplicite e legittime, ed, eventualmente, successivamente trattati in modo che non siano incompatibili con tali finalità (**principio di limitazione della finalità**);
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**principio di minimizzazione dei dati**);
d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (**principio di esattezza**);
e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**principio di limitazione della conservazione**);
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione dalla distruzione o dal danno accidentali (**principio di integrità e riservatezza**).

Considerato che il Responsabile della Protezione dei Dati (di seguito D.P.O.), con nota prot. n. 0091115/23 del 28.10.2023, ha portato all'attenzione della Direzione Generale della ASL di Pescara una serie di condotte commesse da diverse Unità Operative in violazione delle prescrizioni contenute nel GDPR; le condotte evidenziate riguardavano due tipologie di violazione: la mancata pseudonimizzazione dei dati e la mancata cifratura dei dati sanitari inviati a soggetti terzi.

Nella fattispecie il D.P.O. aveva tratto spunto da quanto comunicato alla ASL di Pescara, (in qualità di Titolare del trattamento), dall'Istituto Sperimentale Zooprofilattico di Teramo che, in occasione del ricevimento dei campioni "*provenienti da liquidi biologici e tissutali di origine umana o da materiali connessi alla patologia umana, con particolare riferimento alle informazioni trasmesse dai laboratori o dai reparti ospedalieri*" della ASL di Pescara, rilevava come gli stessi fossero corredati di dati personali identificativi del paziente anziché essere trasmessi ricorrendo a tecniche di pseudonimizzazione e/o di cifratura; fatta eccezione per le prestazioni che richiedono l'intervento della metagenomica, per le quali è fondamentale conoscere i dati anagrafici dei pazienti.

La metodica adottata dalle Unità Operative in questione (trasmissione dei dati identificativi contenenti le richieste di esami) viola il principio di minimizzazione dei dati, alla luce del quale vanno trasmessi i soli dati necessari a raggiungere gli scopi che sorreggono il trattamento; in buona sostanza, per gli esami diagnostici, al di là dei casi espressamente normati (ad es. metagenomica), non è necessario accludere i dati anagrafici dei pazienti ma bisogna pseudonimizzare gli stessi, in modo da evitare la loro attribuzione ad una persona fisica identificata o identificabile.

Preso atto che una **tecnica di pseudonimizzazione** ha lo scopo di sostituire un dato identificativo (es. nomi, codice fiscale, ecc.) con un valore surrogato che spesso è chiamato token, (per quanto di interesse in questa sede, il token è una sequenza di informazioni digitali, registrate in un registro e rappresentative di una persona fisica), il quale deve essere irreversibile senza informazione aggiuntiva e distinguibile dal valore originale; a tale scopo si può ricorrere, ad esempio, ad un codice (in possesso esclusivo di un soggetto autorizzato al trattamento dei dati: SATD o SAT) attraverso cui potere risalire alle generalità del paziente (cd reidentificazione).

A titolo esemplificativo si riportano due esempi di pseudonimizzazione:

Identificativo	**Pseudonimo**
Maria Rossi	15
Antonio Bianchi	18

Altra misura che è obbligatorio adottare in fase di trasmissione dei dati personali particolari (art, 9 GDPR, ad es. i dati sanitari) o giudiziari (art. 10 GDPR) consiste nel ricorso alla tecnica della cifratura dei dati; per l'adozione di tale misura di sicurezza ci si può avvalere del supporto della UOC Sistemi Informativi.

L'adozione di entrambe le misure di sicurezza sopra richiamate (pseudonimizzazione e cifratura dei dati personali) evita, o riduce fortemente, il rischio di violare i diritti e le libertà dei soggetti interessati (in questo caso ci si riferisce ai pazienti per i quali vengono richiesti gli esami), in quanto, ad es., in caso di trasmissione della richiesta di esame/referto, ecc, ad un soggetto diverso da quello interessato (cioè il paziente a cui la documentazione si riferisce), tendenzialmente non si determina un caso di violazione dei dati personali (data breach).

La mancata adozione delle misure tecniche e organizzative consistenti nella pseudonimizzazione e nella cifratura dei dati personali espone la ASL di Pescara (Titolare del trattamento), in caso di violazione dei dati, ad una sanzione amministrativa pecuniaria fino a 10 milioni di euro, (art. 83, paragrafo 4, lettera a) del GDPR).

Si confida nella pedissequa applicazione delle regole sopra riportate con obbligo di sensibilizzare i propri collaboratori (SAT) affinché ne garantiscano il rispetto.

Il mancato ricorso alla pseudonimizzazione dei dati ed alla loro cifratura è da intendersi come violazione degli obblighi richiamati nelle designazioni a SATD e a SAT, con conseguenti responsabilità di natura civile, penale e disciplinare.

IL DIRETTORE AMMINISTRATIVO

Dott.ssa Francesca Rancitelli

IL DIRETTORE GENERALE

Dott. Vero Michitelli