

**Istruzioni sul trattamento dei dati personali nell'ambito del Progetto Presa in Carico
dall'ATS di Bergamo (Titolare) all'Ente ***** (Responsabile del
trattamento)**

ISTRUZIONI E COMPITI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il Gestore, relativamente al percorso di cura dei pazienti cronici e fragili, arruolati nel territorio dell'ATS di Bergamo, quale Responsabile del trattamento dei dati ai sensi dell'art. 28 del Reg. UE 2016/679 è tenuto a:

- compilare e conservare la documentazione sanitaria nel rispetto della normativa vigente, delle indicazioni regionali ed in conformità con i requisiti SISS/FSE;
- comunicare all'ATS tutti i documenti e le informazioni di competenza all'interno del FSE, ai fini del governo della presa in carico, nei termini e con le modalità disposte dalla normativa nazionale e regionale, secondo i format stabiliti e aggiornati nel tempo;
- conservare agli atti il Patto di Cura e i relativi consensi in modalità cartacea e/o dematerializzata.
- gestire il PAI in modalità elettronica, con pubblicazione in FSE, costantemente disponibile ed aggiornato, in base alle modalità di trattamento in FSE e archiviato nel repository del Gestore;
- compilare una scheda informativa contenente i nominativi dei soggetti autorizzati ad accedere ai dati personali ed alle categorie particolari di dati personali del paziente;
- sovrintendere e vigilare che da parte dei operatori incaricati autorizzati ai sensi dell'art. 24 del Reg. UE 2016/679 sia rispettata la normativa vigente in materia di protezione dei dati, le istruzioni impartite e applicate le misure di sicurezza, nonché mantenuto il segreto professionale e gli eventuali obblighi di riservatezza connessi;
- rilasciare al paziente su richiesta le credenziali di accesso ai servizi on line di Regione Lombardia;
- adottare le misure necessarie a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, consentendo l'esercizio di tali diritti, sia direttamente sia in collaborazione con il Titolare, in conformità agli artt. dal 15 al 22 del capo III del Regolamento UE;
- in caso di termine della presa in carico di un paziente, conservare i dati e i documenti in suo possesso in base al manuale della documentazione sanitaria e socio sanitaria di Regione Lombardia, consentendo l'accesso ai dati personali solo agli aventi diritto per legge;
- adottare tutte le misure di sicurezza adeguate al rischio rilevato in conformità all'art. 32 del Regolamento UE 2016/679, nonché delle specifiche disposizioni nazionali e regionali in materia di protezione dei dati personali;

In particolare il gestore, quale responsabile del trattamento, è tenuto ad ottemperare a quanto previsto dall'art. 32 del Regolamento UE 2016/679:

“Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra l'altro:

- a) le pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".

L'ottemperanza a tali obblighi è da considerarsi quale misura minima, fatto salvo che il titolare del trattamento dovrà valutare, anche in base a quanto previsto dagli articoli 28 e 32 del Regolamento UE 2016/679, l'eventuale necessità dell'adozione da parte del gestore di misure ulteriori.

- ai sensi dell'art. 33 c. 2 del Regolamento UE 2016/679, segnalare al Titolare e al Responsabile del trattamento del sistema informativo di supporto regionale Lispa Spa, senza ingiustificato ritardo e comunque entro le 36 ore dal momento in cui ne è venuto a conoscenza, ogni violazione di dati personali e di incidenti che possano compromettere la sicurezza dei dati, e a seconda dei casi, adottando direttamente e/o proponendo l'adozione di tempestive e adeguate misure di sicurezza;
- redigere e aggiornare periodicamente, in base alla tipologia e natura dei dati trattati, un documento di analisi dei rischi effettivi del trattamento e sulla efficacia delle relative misure adottate;
- curare e tenere a disposizione del Titolare e dell'Autorità di controllo, il Registro delle operazioni di trattamento dei dati personali effettuati per conto del Titolare ed il Registro delle violazioni dei dati;
- dimostrare e attestare la conformità del trattamento alle disposizioni normative ed alle misure disposte dal Titolare, garantendo la tracciabilità delle azioni compiute e la relativa documentabilità;
- informare, consultare e collaborare con il Titolare per tutte le questioni rilevanti anche ai fini di legge (es. richieste del Garante, delle Autorità Pubbliche, degli interessati, valutazioni di impatto, data breach...) e per la loro risoluzione;
- collaborare con il Garante della protezione dei dati personali nello svolgimento delle sue funzioni, riscontrando le eventuali richieste e attuando i provvedimenti adottati dallo stesso, o supportando il Titolare in tali adempimenti;
- comunicare l'adesione a codici di condotta e/o a schemi di certificazioni, sigilli e marchi, che avranno l'efficacia prevista dal Regolamento UE, ai sensi degli artt. 40 e 42.
- comunicare i dati di contatto del Responsabile della protezione dei dati personali;
- garantire che le persone a qualsiasi titolo autorizzate a trattare i dati a carattere personale (dipendenti, consulenti, collaboratori, altri soggetti):
 - a. rispettino la riservatezza sull'attività svolta;
 - b. ricevano, prima dell'inizio delle attività di trattamento, la necessaria formazione in materia di protezione dei dati a carattere personale e le istruzioni di cui al presente allegato.

DIVIETI

Al Gestore – Responsabile è vietato:

- diffondere le categorie particolari di dati personali di cui all'art. 9 del Reg. UE 2016/679;
- comunicare e/o trasferire i dati personali a terzi senza previa informazione e/o autorizzazione del Titolare;
- effettuare trattamenti non finalizzati all'esecuzione dell'incarico/contratto affidato e/o nuovi trattamenti non previamente autorizzati dal Titolare.

La designazione a Responsabile del trattamento non comporta diritti a specifici compensi e/o indennità, poiché l'attività di trattamento è necessariamente intrinseca all'adempimento dell'attività contrattuale.

La designazione a responsabile del trattamento ha la medesima durata del presente contratto.