SCHEMA di Contratto tra il Titolare del trattamento dei dati personali e il Responsabile del trattamento Ente del Terzo Settore (ETS) ai sensi dell'art. 28 del Regolamento UE 2016/679.

TRA

L'Azienda Sanitaria Territoriale dei Sette Laghi, con sede legale in Varese, viale Borri n. 57, Cod.Fisc./P.IVA n. 03510050127, (di seguito il "**Titolare**" o "ASST dei Sette Laghi"), in persona del Direttore Generale individuato quale legale rappresentante *pro tempore*

e

L'Ente del Terzo Settore (ETS) , con sede legale in…….. iscritta al Registro del Terzo Settore della ASST dei Sette Laghi; in persona del suo legale rappresentante *pro tempore*, in qualità di Responsabile del trattamento dei dati (di seguito il "**Responsabile del trattamento**" o il "Fornitore"),

denominati congiuntamente le "**Parti**";

PREMESSO CHE

- in data l'ETS, previa istruttoria, risulta iscritto al Registro del Terzo Settore della ASST dei Sette Laghi;
- **l'ETS**, nell'ambito dell'esecuzione delle proprie attività come dettagliate all'atto dell'iscrizione al Registro, svolge in tutto o in parte operazioni di trattamento di dati personali (di seguito "Dati") le cui decisioni in ordine ai mezzi, alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sono stabiliti dal Titolare;
- l'articolo 16 ("Disposizioni in materia di tutela dei dati personali") del "Regolamento per la collaborazione tra associazioni di volotariato e azienda socio-sanitaria territoriale dei Sette Laghi di Varese", vincola l'ETS al rispetto delle norme vigenti in materia di protezione dei dati personali;
- dal 25 maggio 2018 è applicato il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, che ha ad oggetto la tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito definito anche "**GDPR**" o "Regolamento");
- dal 19 settembre 2018 è in vigore il decreto legislativo 10 agosto 2018 n. 101, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679, decreto che ha apportato sostanziali modifiche al decreto legislativo 30 giugno 2003, n. 196 (di seguito "**Codice Privacy e s.m.i.**");
- l'art. 4, paragrafo 1, n. 1, del GDPR, definisce «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («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;

- l'art. 4, paragrafo 1, n. 2, del GDPR, definisce «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- l'art. 4, paragrafo 1, n. 7, del GDPR definisce il «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- l'art. 4, paragrafo 1, n. 8, del GDPR, definisce il «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- l'art. 28, paragrafo 1, del Regolamento stabilisce che:
  - «*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*».
  - l'art. 28, paragrafi 3 e 9, del Regolamento impone che i trattamenti di dati autorizzati dal Titolare al Responsabile: "*siano disciplinati da un **contratto** o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri*", stipulato in forma scritta o in formato elettronico, "***che vincoli il responsabile del trattamento al titolare del trattamento** e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento";*
  - a norma dell'art. 81, paragrafo 1, del Regolamento: "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*" e che ai sensi del successivo paragrafo 2: "***un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento***", salvo che dimostri che l'evento dannoso non gli è in alcun modo imputabile

CONSIDERATO CHE

- **le parti** con la sottoscrizione del presente contratto intendono regolare i loro reciproci rapporti in relazione alle attività di trattamento di dati personali effettuate dal Responsabile per conto del Titolare del trattamento;

- con la sottoscrizione del presente contratto, nel quadro delle loro relazioni contrattuali, le parti si impegnano a **rispettare** la normativa europea e nazionale in vigore sul trattamento dei dati personali;

- Il Responsabile, sottoscrivendo il presente accordo, dichiara e garantisce di possedere la

competenza e le **conoscenze tecniche** in relazione alle finalità e modalità delle operazioni di trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza e integrità dei dati trattati, nonché alla normativa applicabile in materia di tutela dei dati personali;

- L'ETS , in qualità di Responsabile del trattamento dei dati, si assume il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni normative vigenti in materia e di osservare scrupolosamente quanto in esse previsto, nonché le istruzioni impartite dal Titolare.

RILEVATO CHE

- l'ASST dei Sette Laghi ha verificato che l'ETS possa soddisfare i requisiti generali e di sicurezza e che, in particolare, possiede competenze e conoscenze tecniche in relazione alle finalità e modalità di trattamento, alle misure tecniche ed organizzative da adottare a tutela dei diritti degli interessati, e monitora il rispetto della normativa europea e nazionale applicabile in materia di protezione dei dati personali (inclusi i Provvedimenti del Garante per la protezione dei dati e dell'EDPB).

Tutto quanto sopra premesso, considerato e rilevato, le Parti convengono e stipulano quanto segue:

1. OGGETTO E FINALITÀ DEL TRATTAMENTO

Il Responsabile effettuerà trattamenti di dati personali per conto del Titolare all'unico **scopo di espletare le attività e i servizi** oggetto del rapporto di cui in Premessa.

2. DATI TRATTATI E CATEGORIE DI INTERESSATI COINVOLTI

I dati trattati dal Responsabile, per conto del Titolare, sono eslusivamente i dati strettamente necessari per l'espletamento delle attività delle ETS definite all'atto dell'iscrizione di cui in Premessa.
In particolare, l'ETS tratta per conto dell'ASST dei Sette Laghi:

- i dati del personale dell'ASST con cui l'ETS entra in contatto per l'espletamento della propria attività;
- i dati di pazienti e dei loro familiari comunicati dall'ASST per lo svolgimento delle attività dell'ETS;
- i dati di pazienti e loro familiari direttamente comunicati dagli Interessati agli operatori dell'ETS.

Il trattamento ha ad oggetto, di regola, dati personali di tipo identificativo e può estendersi a dati cd. "particolari" ex art. 9 GDPR dei pazienti dell'ASST solo nelle ipotesi in cui la loro conoscenza sia strettamente necessaria e pertinente all'attività dell'ETS.

3. DURATA DEL TRATTAMENTO

Il trattamento avrà durata pari al periodo di iscrizione al Resgistro Aziendale del Terzo Settore.

Le parti convengono inoltre che il trattamento cesserà al verificarsi di una qualsiasi causa di cancellazione dal Registro del Terzo Settore.

4. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento s'impegna a:

- Fornire al Responsabile del trattamento i dati previsti al punto 2 delle presenti clausole;
- Documentare per iscritto tutte le ulteriori istruzioni riguardanti il trattamento dei dati da parte del Responsabile del trattamento;
- Vigilare, in anticipo e durante la durata del rapporto, il rispetto degli obblighi previsti dal Regolamento europeo sulla protezione dei dati, nonché dalla normativa complessivamente indicata in Premessa, da parte del Responsabile del trattamento;
- Supervisionare le attività di trattamento effettuate per dare esecuzione alle attività oggetto del rapporto, comprese le revisioni e le ispezioni da parte del Responsabile del trattamento.

Il Titolare del trattamento determina le finalità e i mezzi del trattamento dei dati personali trattati per suo conto dal Responsabile e mette in atto, con l'ausilio del Responsabile, misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente alla normativa europea e nazionale.
Il Titolare e il Responsabile – sulla base delle istruzioni impartite dal Titolare – provvedono a riesaminare e aggiornare le misure tecniche e organizzative impiegate, qualora necessario.
Qualora, ai fini dell'adeguamento alla normativa in materia di protezione dei dati, si rendano necessarie ulteriori attività o misure specifiche, o nel caso di modifiche delle attività oggetto del rapporto che comportino impatto sul trattamento dei dati personali, ove necessario, il Titolare trasmetterà al Responsabile ulteriori istruzioni in merito alle finalità, modalità e procedure per l'utilizzo e il trattamento dei dati personali, e concorderà con il Responsabile le misure tecniche e organizzative più idonee.

5. REFERENTI, AUTORIZZATI AL TRATTAMENTO E AMMINISTRATORI DI SISTEMA

Il Titolare chiede al Responsabile di individuare e nominare gli autorizzati al trattamento dei dati e gli eventuali amministratori di sistema vincolandoli alle istruzioni impartite dal Titolare del trattamento e dal Responsabile.
Il Responsabile si impegna a garantire che le persone individuate come sopra agiscano sotto la propria autorità, esclusivamente sulla base delle adeguate istruzioni fornite dal Titolare e che siano state adeguatamente formate in relazione ai loro compiti e responsabilità, nonché vincolate ad un obbligo di riservatezza.
Il Responsabile si impegna a mettere a disposizione del Titolare un elenco costantemente aggiornato dei nominativi dei soggetti sopra indicati.

6. OBBLIGHI DEL RESPONSABILE

Il **Responsabile** del trattamento dei dati personali, operando nel rispetto della normativa europea e nazionale sul trattamento dei dati personali deve attenersi ai seguenti **compiti ed istruzioni**:

1. Trattare i dati **solo per la finalità o le finalità** sopra specificate e per l'esecuzione delle attività definite all'atto dell'iscrizione al Registro del Terzo Settore;

2. Garantire la riservatezza dei dati personali trattati nell'ambito delle attività suddetta, in quanto informazioni riservate nella titolarità dell'ASST.

In virtù di tale obbligo, il Responsabile del trattamento:

a) non dovrà in alcun caso comunicare i dati a terzi, a meno che ciò non sia necessario per l'assolvimento di un obbligo di legge, previa comunicazione al Titolare;
b) non dovrà in alcun modo trasferire dati personali verso soggetti terzi oppure ad un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione Europea o nazionale.

   Fuori dai predetti casi e fatto salvo il trasferimento ad ulteriori Responsabili del trattamento autorizzati dal Titolare, il Responsabile è tenuto a chiedere specifica autorizzazione al Titolare nel caso in cui riceva richiesta o intimazione di comunicare informazioni personali o inerenti alle operazioni di trattamento regolato nel presente contratto (da parte di una pubblica autorità o da parte dell'autorità giudiziaria).

3. Non ricorrere ad un **altro Responsabile** senza aver ricevuto una previa autorizzazione scritta, generale o specifica, da parte del Titolare del trattamento.
   Ove necessario, impegnarsi a selezionare esclusivamente **Sub-responsabili** che presentino **garanzie** sufficienti, in conformità a quanto previsto dalla normativa in materia di protezione dei dati personali, alla messa in atto di misure tecniche e organizzative appropriate, affinché il trattamento risponda alle esigenze del Regolamento europeo sulla protezione dei dati. Trasmettere ai **Sub-responsabili** individuati i medesimi obblighi da esso assunti nei confronti del Titolare, fermo che il Sub-responsabile non adempia alle proprie obbligazioni in materia di protezione dei dati, il Responsabile del trattamento risponderà per intero davanti al Titolare del trattamento dell'inadempimento del Sub-responsabile;

4. attenersi alle **istruzioni** documentate provenienti dal Titolare del trattamento. Il Responsabile si impegna a informare immediatamente il Titolare nel caso in cui ritenga che una istruzione costituisca una violazione del GDPR o di altre disposizioni nazionali o dell'Unione, relative alla protezione dei dati personali;

5. informare nel caso in cui sia tenuto a procedere ad un trasferimento di dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione Europea o delle leggi dello stato membro al quale è sottoposto il Titolare, prima del trattamento, sempre che le leggi interessate vietino tale informazione per rilevanti motivi di interesse pubblico;

6. garantire che i propri **le persone autorizzate al trattamento** (di seguito "Autorizzati") e gli eventuali **amministratori di sistema** siano designati per iscritto, con un atto che stabilisca le modalità di accesso ai dati e le attività di competenza, nonché che le stesse siano vincolate, tramite impegno formale, da un obbligo di **riservatezza**.
   Il Responsabile si impegna a verificare l'adempimento da parte delle persone autorizzate del suddetto obbligo di riservatezza o che le stesse siano sottoposte a un obbligo legale appropriato di segretezza. Il Responsabile si impegna inoltre a sottoporre le persone autorizzate al trattamento alla necessaria formazione in materia di protezione dei dati personali.
   Il Responsabile si impegna altresì a comunicare annualmente l'elenco nominativo degli autorizzati al trattamento con relativi profili autorizzativi, nonché a comunicare tempestivamente al Titolare del trattamento qualsiasi variazione ai profili autorizzativi concessi per motivi di sicurezza.

7. comunicare al Titolare del trattamento **il nome e i dati del proprio Responsabile della protezione dei dati**, qualora ne abbia designato uno conformemente all'articolo 37 del GDPR;

8. scegliere gli eventuali **amministratori di sistema** tra i soggetti in grado di garantire il rispetto della normativa in materia di protezione dei dati personali e nominare e istruire gli amministratori di sistema individualmente, elencando espressamente gli ambiti di operatività consentiti a ciascun amministratore in relazione al proprio profilo di autenticazione;
   In ogni caso, il Responsabile si impegna a conformarsi a quanto stabilito dal Provvedimento del Garante per la protezione dei dati personali "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008*", pubblicato in G.U. n. 300 del 24 dicembre 2008 e successive modifiche;

9. tenere conto, utilizzando i materiali, i prodotti, le applicazioni o i servizi, dei principi di **protezione dei dati by design** e della **protezione dei dati by default;**

10. assistere il Titolare del trattamento, con misure tecniche e organizzative adeguate, nelle seguenti attività:
    - nel riscontro alle **legittime richieste formulate dagli interessati nell'esercizio dei diritti** che gli sono riconosciuti dal GDPR (artt. 15-22), fornendo tutte le informazioni eventualmente necessarie a tal fine e comunicando al Titolare senza ritardo, e comunque entro 2 gg dal momento della ricezione, qualunque istanza ricevuta per l'esercizio dei diritti degli interessati inerente ai trattamenti eseguiti per conto del Titolare medesimo, allegando copia della richiesta;
    - nella gestione di eventuali violazioni di dati personali, ai sensi degli artt. 33 e 34 del GDPR, comunicando, senza ritardo e comunque entro 36 ore dal momento in cui ne è venuto a conoscenza, al Titolare del trattamento, qualsiasi violazione dei dati personali di cui è venuto a conoscenza, nel rispetto dell'art. 33 del Reg. GDPR e delle istruzioni di volta in volta fornite dal Titolare in ottemperanza alle policy dallo stesso adottate. Tale comunicazione è accompagnata da ogni documentazione utile per permettere al Titolare del trattamento, se necessario, di notificare questa violazione all'autorità di controllo competente;
    - nella valutazione d'impatto dei trattamenti previsti sulla protezione dei dati, di cui all'art. 35 del GDPR;
    - nella consultazione preventiva dell'autorità di controllo, nelle ipotesi disciplinate dall'art. 36 del GDPR.

11. **cancellare i dati personali** alla scadenza dell'iscrizione al Registro del Terzo Settore, salvo diversa disposizione normativa. Una volta distrutti, il Responsabile del trattamento deve documentare al Titolare per iscritto la distruzione;

12. provvedere, ogni qualvolta si raccolgano dati (foto, video, nomi e cognomi, ecc…), a fornire, ove necessaria, un'**informativa** ai soggetti Interessati che presenti tutti i requisiti prescritti dagli artt. 13 e 14 del GDPR e dalla normativa vigente in materia. La formulazione e il formato dell'informativa, nei casi in cui la stessa abbia ad oggetto trattamenti di cui al presente accordo, debbono essere convenuti con il Titolare del trattamento, prima della

raccolta dei dati;

13. **conservare** i dati trattati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono raccolti e successivamente trattati come da privacy policy del Titolare del trattamento;

14. consentire ed agevolare il Titolare nel **controllare in qualsiasi momento le operazioni sul trattamento di dati personali svolte per conto di quest'ultimo**, ivi comprese le misure di sicurezza impiegate dal Responsabile per la tutela dei dati, anche tramite appositi audit da concordarsi preventivamente nel rispetto dei reciproci impegni e necessità.

7. RESPONSABILITÀ DEL RESPONSABILE

Ai sensi del GDPR il Responsabile risponde del pagamento di sanzioni amministrative pecuniarie irrogate dalle autorità di controllo, alle condizioni previste dal medesimo Regolamento.

In particolare, ai sensi dell'art. 28, paragrafo 10 del GDPR, fatti salvi gli articoli 82, 83 e 84, il Responsabile che violi il GDPR, determinando le finalità e i mezzi del trattamento, verrà considerato titolare del trattamento in questione.

Il Responsabile inoltre, ai sensi dell'art. 82 del GDPR, risponde del danno patrimoniale e non patrimoniale cagionato dal trattamento, se non ha adempiuto agli obblighi specificatamente diretti ai responsabili del trattamento previsti dalla normativa o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni impartite dal Titolare del trattamento.

Il Responsabile risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza, nonché di qualsiasi violazione delle istruzioni impartite per iscritto dal Titolare del trattamento.

Infine, ai sensi dell'art. 28, paragrafo 4 del GDPR, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi gravanti sul Sub-responsabile nel caso in cui quest'ultimo ometta di adempiere ai propri obblighi in materia di protezione dei dati.

8. MANLEVA

Il Responsabile si impegna a manlevare e a risarcire il Titolare per qualsivoglia conseguenza sanzionatoria o risarcitoria che possa derivare da un proprio comportamento in contrasto alla normativa sulla tutela dei dati personali, ovvero contrario alle presenti istruzioni o a quelle che verranno impartite successivamente dal Titolare del trattamento.
Nelle ipotesi sopra delineate il Titolare si riserva il diritto di risolvere il rapporto in essere, tramite l'invio di una comunicazione scritta al Responsabile. Resta fermo, in ogni caso, il risarcimento dei danni subiti.

9. PERSONALITA' DELLA NOMINA

L'incarico di Responsabile del trattamento dei dati **non è suscettibile di delega.** Esso **decade** automaticamente in qualsiasi ipotesi in cui venga meno il rapporto che lo lega con il Titolare del trattamento.
In caso di **cessazione,** il Responsabile si impegna a cessare qualsiasi operazione di trattamento di dati personali per conto del Titolare, a provvedere alla **distruzione** dei dati, fornendone adeguata attestazione, eccettuate eventuali esigenze di conservazione in adempimento di obblighi normativi, di cui andrà data contestuale attestazione al Titolare.
Resta inteso che il presente contratto non comporta alcun diritto ad uno specifico **compenso e/o indennità**, giacché gli obblighi ivi contenuti sono imposti dal Regolamento UE 2016/679, in relazione alla gestione di dati personali per conto del Titolare.
Le parti riconoscono che le previsioni di cui al presente accordo sono espressione delle libere trattative intercorse tra le stesse parti e non necessitano di specifica sottoscrizione, *ex* art. 1341 cod. civ.

10. LEGGE APPLICABILE E FORO COMPETENTE

Il presente Contratto è regolato dalla legge italiana.
Per qualsiasi controversia dovesse sorgere in relazione al presente Contratto, sarà competente in via esclusiva il Tribunale di Varese.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Varese, _____

IL TITOLARE DEL TRATTAMENTO	**IL RESPONSABILE DEL TRATTAMENTO**
IL DIRETTORE GENERALE DI ASST SETTE LAGHI	*IL LEGALE RAPPRESENTANTE PROTEMPORE DELL'ETS*
_____	_____