193265
Decreti del Presidente - **Parte 1 - Anno 2022**

Provincia Autonoma di Trento

DECRETO DEL PRESIDENTE DELLA PROVINCIA
del 30 giugno 2022, n. 10-67/Leg.

Regolamento concernente la medicina di iniziativa nel servizio sanitario provinciale di attuazione dell'art. 4, comma 1 ter della legge provinciale n. 16 del 2010

Continua >>>

PROVINCIA AUTONOMA DI TRENTO

Prot. n.

DECRETO DEL PRESIDENTE N. 10-67/Leg. DI DATA 30 Giugno 2022

OGGETTO:
Regolamento concernente la medicina di iniziativa nel servizio sanitario provinciale di attuazione dell'art. 4, comma 1 ter della legge provinciale n. 16 del 2010.

IL PRESIDENTE DELLA PROVINCIA

- visto l'articolo 53 del decreto del Presidente della Repubblica 31 agosto 1972, n. 670, recante "Approvazione del testo unico delle leggi costituzionali concernenti lo Statuto speciale per il Trentino-Alto Adige", ai sensi del quale il Presidente della Provincia emana con proprio decreto i regolamenti deliberati dalla Giunta provinciale;
- visto l'articolo 54, comma 1, numero 1, del medesimo del decreto del Presidente della Repubblica secondo il quale la Giunta provinciale è competente a deliberare i regolamenti per l'esecuzione delle leggi approvate dal Consiglio provinciale;
- visto l'articolo 4 della legge provinciale sulla "Tutela della salute in provincia di Trento" che al comma 1 bis stabilisce che "la Provincia riconosce e promuove la medicina di iniziativa quale modello assistenziale del sistema sanitario provinciale finalizzato alla diagnosi precoce e alla prevenzione, sia primaria che secondaria, delle patologie croniche e alla conseguente attivazione di interventi mirati al cambiamento degli stili di vita e alla presa in carico integrata e multidisciplinare";
- visto il Regolamento (UE) 2016/679, del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- visto il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (decreto legislativo n. 196 del 2003, come modificato dal decreto legislativo 10 agosto 2018, n. 101);
- visto l'art. 7 del decreto-legge n. 34 del 2020 recante "Metodologie predittive dell'evoluzione del fabbisogno di salute della popolazione", come novellato in sede di conversione del decreto-legge n. 139 del 2021;
- su conforme deliberazione della Giunta provinciale n. 1006 di data 7 giugno 2022, con la quale è stato approvato il "Regolamento concernente la medicina di iniziativa nel servizio sanitario provinciale di attuazione dell'art. 4, comma 1 ter della legge provinciale n. 16 del 2010";

e m a n a

il seguente regolamento:

Art. 1
Definizioni

1. Ai fini del presente regolamento si applicano le definizioni di cui all'articolo 4 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
2. In aggiunta a quanto previsto al comma 1, ai fini del presente regolamento, si intende per:

a) "medicina di iniziativa": il modello assistenziale della sanità finalizzato alla prevenzione e diagnosi precoce delle patologie croniche e alla conseguente attivazione di interventi mirati al cambiamento degli stili di vita e alla presa in carico integrata e multidisciplinare degli assistiti e assistibili residenti in provincia di Trento, realizzato ai fini di medicina preventiva, diagnosi, terapia, assistenza sanitaria e sociale, nonché di elaborazione delle informazioni statistiche a supporto delle attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
b) "interessato": il soggetto assistito o assistibile dal servizio sanitario provinciale;
c) "profilo di rischio di fragilità": espressione del rischio per problemi di salute la cui ospedalizzazione o progressione sono potenzialmente evitabili, attraverso cure appropriate a livello territoriale.

Art. 2
Oggetto del regolamento

1. La Provincia autonoma di Trento (di seguito Provincia) riconosce e promuove la medicina di iniziativa quale modello assistenziale del sistema sanitario provinciale finalizzato alla diagnosi precoce e alla prevenzione, sia primaria che secondaria, delle patologie croniche e alla conseguente attivazione di interventi mirati al cambiamento degli stili di vita e alla presa in carico integrata e multidisciplinare.
2. Ai sensi dell'art. 4 comma 1 ter della legge provinciale 16 del 2010, "Legge sulla tutela della salute in Provincia di Trento", il presente regolamento individua i tipi di dati personali che possono essere trattati, le operazioni eseguibili, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi degli interessati con riferimento all'attività di stratificazione legata al modello assistenziale della medicina di iniziativa, per il perseguimento di motivi di interesse pubblico rilevante previsti dall'articolo 2-sexies del decreto legislativo n. 196/2003 e ss.mm.ii., comma 2, lettera u) e v) e del paragrafo 2, lettera g) dell'articolo 9 del Regolamento (UE) 2016/679 "Trattamento di categorie particolari di dati personali". Il presente regolamento disciplina altresì le specifiche finalità perseguite.
3. Per l'attività di cui al comma 2 l'Azienda provinciale per i servizi sanitari (di seguito APSS o Azienda) tratta i dati generati provenienti dalle fonti di cui all'articolo 6 del presente regolamento e secondo le modalità individuate dall'articolo 7 nel rispetto delle misure di sicurezza di cui all'articolo 10.
4. Ai sensi dell'art. 4, comma 1 quater della legge provinciale n. 16 del 2010, l'eventuale trattamento effettuato successivamente alla stratificazione, sulla base di tale modello, per finalità di cura, al fine di realizzare, con riferimento a specifiche patologie, un profilo sanitario di rischio, richiede necessariamente la preventiva acquisizione del consenso informato da parte dell'interessato, in quanto trattamento automatizzato non strettamente necessario per finalità di cura dell'interessato e, quindi, quale trattamento autonomo rispetto a quello principale finalizzato alla cura.

Art. 3
Finalità specifiche del trattamento di dati

1. Nell'ambito delle finalità di interesse pubblico rilevante di cui all'articolo 2, la medicina d'iniziativa mira sia alla prevenzione, sia al miglioramento della gestione delle malattie croniche in ogni loro stadio, con effetti positivi attesi sia per la salute dei cittadini che per la sostenibilità stessa del sistema e, quindi, ad una presa in carico proattiva a beneficio degli assistiti. L'obiettivo dell'identificazione precoce dei cittadini a rischio di cronicità/fragilità, per definire

interventi mirati di medicina di iniziativa, si raggiunge attraverso la stratificazione dell'intera popolazione sulla base del profilo di rischio di fragilità, espresso in termini di rischio per problemi di salute. La stratificazione viene effettuata attraverso algoritmi deterministici basati su tecniche di analisi statistica dei dati gestiti nell'ambito dei diversi archivi del sistema informativo aziendale.

2. La differenziazione, quale risultato della stratificazione, risulta indispensabile per:
   - analizzare e valutare ai fini di governo lo stato di salute dell'intera o di gruppi della popolazione sulla base del profilo di rischio di fragilità, espresso in termini di rischio per problemi di salute, al fine di migliorare la pianificazione e il governo degli interventi sociosanitari dell'Azienda e la loro efficacia ed efficienza rispetto alla distribuzione territoriale;
   - definire le strategie e gli interventi più appropriati di medicina di iniziativa rispetto a quei sottogruppi di popolazione che potrebbero maggiormente beneficiarne, per ottimizzare il trattamento multidisciplinare e personalizzare l'assistenza e il Piano di cura, nel rispetto del principio di equità e di centralità del paziente e delle sue scelte;
   - valutare l'appropriatezza, l'efficacia e l'efficienza dell'assistenza erogata e delle attività di prevenzione, anche con riferimento a specifiche patologie o problematiche sanitarie, nonché anche attraverso la caratterizzazione dell'esposizione a fattori di rischio;
   - ridurre gli interventi inappropriati e conseguentemente contenere la spesa sanitaria.

Art. 4
Titolare del trattamento dei dati

1. L'APSS è il Titolare del trattamento dei dati effettuato ai fini dell'attività di medicina d'iniziativa.

Art. 5
Tipi di dati personali trattati

1. Per il perseguimento delle finalità di cui all'articolo 3, il Titolare tratta dati personali e dati relativi alla salute.
2. Sono oggetto del trattamento le seguenti tipologie di dati estratte dalle fonti riportate nell'articolo 6:
   - dati anagrafici, sesso, età, comune di residenza/domicilio dell'assistito;
   - presenza e tipo di esenzioni per patologia e/o reddito;
   - dati di ricovero in regime di urgenza, ordinario, day hospital/day surgery, cure intermedie;
   - visite, prestazioni, assistenza a pazienti che accedono al Pronto soccorso (PS)/Osservazione Breve (OB);
   - prestazioni specialistiche erogate in regime ambulatoriale;
   - farmaci erogati da farmacie territoriali, in modalità diretta o per conto, in regime di ricovero;
   - prestazioni di medicina generale o da pediatri di libera scelta;
   - prestazioni erogate a pazienti dell'area della salute mentale - psichiatria, neuropsichiatria, psicologia;
   - visite e prestazioni erogate a domicilio;
   - assistenza e prestazioni erogate a non autosufficienti, in regime residenziale e semiresidenziale;
   - assistenza e prestazioni per pazienti con disturbi del comportamento;
   - assistenza e prestazioni a pazienti in hospice;

- ricoveri, prestazioni, farmaci erogati a residenti in provincia di Trento da strutture nazionali extra provincia di Trento o da strutture internazionali;
- prestazioni erogate presso le terme;
- prestazioni riabilitative erogate in regime ambulatoriale;
- valutazioni multidisciplinari svolte per accedere a servizi sanitari;
- dati delle prenotazioni di prestazioni specialistiche o di ricovero;
- dati relativi a dispositivi medici e in vitro assegnati ai pazienti;
- dati relativi all'assistenza integrativa e protesica erogata ai pazienti;
- dati relativi a patologie infettive e diffusive, tossinfettive, ad esclusione dei dati relativi all'infezione HIV;
- dati relativi ad attività trasfusionali singole o cicliche;
- attività vaccinali;
- informazioni relative a reazioni avverse a farmaci e degli eventi avversi;
- informazioni relative alle diagnosi e ai trattamenti e prestazioni erogati a pazienti contenute nei registri di patologia tumorale, malattie rare, malformazioni congenite, insufficienza renale cronica, trattamento dialitico sostitutivo, trapianti.

3. I suddetti dati sanitari sono costituiti in generale da diagnosi, procedure, trattamenti, prestazioni, esami, analisi, dispensazione di farmaci e dispositivi, valutazioni clinico/sanitarie, certificazione di stati e condizioni clinico/sanitarie, erogazione di prestazioni clinico/sanitarie nei vari regimi (di ricovero, in strutture residenziali e semiresidenziali, di comunità etc.), erogazione di assistenza infermieristica sul territorio e a domicilio, iscrizione nei registri di patologia, altre condizioni clinico/sanitarie desumibili dagli archivi e riconducibili comunque al singolo iscritto all'anagrafe assistibili.
4. Il modello tratta i dati personali degli interessati raccolti nelle fonti di cui all'articolo 6 degli ultimi 10 anni.
5. Per le finalità di cui al presente regolamento non è previsto il trattamento di dati personali cosiddetti "super sensibili", quali ad esempio quelli relativi a dipendenze, all'interruzione volontaria di gravidanza, all'accertamento dell'infezione da HIV e alle disposizioni sulla fecondazione artificiale. Tali dati vengono infatti codificati nelle relative fonti con modalità tecniche che consentono di escluderli dal caricamento nel sistema utilizzato per la stratificazione.
6. I dati sono trattati in forma pseudonimizzata, nel rispetto dei principi di esattezza, integrità, disponibilità, riservatezza già a partire dai trattamenti che alimentano le fonti dati, garantendo agli interessati l'esercizio dei diritti ai sensi del Regolamento UE 2016/679.
7. Dagli archivi di cui all'articolo 6 verranno estratte in forma pseudonimizzata, secondo le tecniche indicate nel punto 6 del disciplinare tecnico allegato, le seguenti tipologie di dati personali: dati comuni e dati relativi alla salute.
8. Per le finalità di cui all'articolo 3, i risultati della stratificazione verranno utilizzati in forma aggregata.

Art. 6
Fonti dei dati

1. Il trattamento, per le finalità di cui all'articolo 3, ha ad oggetto i dati personali e particolari provenienti dai registri elencati all'art. 14 della legge provinciale n. 16 del 2010 e dai diversi archivi del sistema informativo della Provincia e dell'Azienda, di seguito elencati:
   - Anagrafe provinciale assistibili;
   - Archivio delle esenzioni;

- Archivio dei ricoveri ospedalieri;
- Archivio dei ricoveri delle cure intermedie;
- Archivio degli accessi e dell'attività di pronto soccorso, compresa l'Osservazione breve (OB);
- Archivio dell'assistenza specialistica ambulatoriale;
- Archivio farmaceutica territoriale;
- Archivio distribuzione diretta farmaci e distribuzione per conto;
- Archivio della terapia e somministrazione in reparto;
- Archivio gestione economica dei medici di medicina generale e dei pediatri di libera scelta;
- Archivio dell'assistenza alla salute mentale, psichiatrica, neuropsichiatrica, psicologica;
- Archivio dei pazienti in assistenza domiciliare integrata;
- Archivio dell'assistenza erogata presso le strutture sanitarie e sociosanitarie residenziali e semiresidenziali per non autosufficienti;
- Archivio degli interventi erogati presso le strutture hospice;
- Archivio della mobilità sanitaria interregionale passiva e attiva;
- Archivio della mobilità sanitaria internazionale passiva e attiva;
- Archivio dell'assistenza e delle prestazioni termali;
- Archivio delle prestazioni riabilitative;
- Archivio delle valutazioni multidisciplinari;
- Archivio delle prenotazioni specialistiche e di ricovero;
- Archivi dei consumi di risorse dispositivi medici, diagnostica in vitro ecc.;
- Archivio dell'assistenza integrativa e protesica;
- Archivi delle malattie infettive e diffusive e tossinfezioni alimentari;
- Archivio dell'attività immuno-trasfusionale;
- Archivi delle vaccinazioni;
- Archivi di farmacovigilanza, farmaco sorveglianza e dispositivo vigilanza, delle reazioni avverse;
- Archivio dei dializzati e dell'assistenza in dialisi;
- Registro dell'assistenza al parto;
- Registro trapianti.

2. Le fonti individuate per l'effettuazione della stratificazione sono di quattro tipi:
   - fonti in cui sono disponibili diagnosi in formato ICD-IX, ICD-X (International Classification of Primary Care) e ICPC (International Classification of Primary Care) es. ricoveri, esenzione ticket per patologia, iscrizione a registri di patologia;
   - fonti per cui è disponibile la prescrizione di farmaci, es. flussi della farmaceutica territoriale, della distribuzione diretta e per conto, della terapia e somministrazione in reparto;
   - fonti per cui è determinabile l'accesso a servizi sanitari o condizioni di salute (es. accessi di PS, accessi a strutture residenziali o semiresidenziali);
   - fonti per cui è disponibile il codice LOINC (Logical Observation Identifiers Names and Codes), sistema di codifica standardizzato per la descrizione univoca di osservazioni cliniche e di laboratorio.

Art. 7
Trattamento e comunicazione dei dati

1. APSS svolge sui suddetti dati le seguenti operazioni di: raccolta, registrazione, organizzazione, strutturazione, stratificazione, conservazione, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, cancellazione, pseudonimizzazione, anonimizzazione, elaborazione con modalità informatizzate tramite metodologie e tecniche di analisi statistico-probabilistica.

Le predette operazioni sono effettuate in maniera tale per cui in nessun caso possano essere assimilate a processi decisionali automatizzati. Le decisioni prese al riguardo della persona non sono basate esclusivamente su elaborazioni di tipo automatico; tali elaborazioni sono infatti svolte per fornire informazioni più complete possibili al professionista sanitario riguardo lo stato di salute dell'interessato, a supporto delle decisioni che il professionista deve assumere nella fase di presa in carico precoce dell'assistito.

2. In particolare, la stratificazione viene utilizzata per misurare lo stato di salute della popolazione, raggruppando le persone in strati clinicamente coerenti atti ad individuare il rischio presente di eventi avversi o di consumo di risorse sanitarie; la stratificazione consente l'individuazione di gruppi omogenei di persone affette da comorbilità, multi morbilità, multiprescrizione e ne favorisce la presa in carico precoce - medicina di iniziativa - per migliorare la qualità dell'assistenza sanitaria e socio-sanitaria e l'outcome degli interventi assistenziali.

   Le macro-fasi del trattamento e di elaborazione delle informazioni sono le seguenti:
   - individuazione di fonti, flussi e basi dati in cui sono presenti informazioni delle tre tipologie descritte;
   - per ogni fonte, individuazione dei dati riferibili a diagnosi codificate e dei dati relativi ad accessi e utilizzi di servizi sanitari, nonché le informazioni relative all'uso di farmaci;
   - estrazione dei dati strettamente necessari all'alimentazione del sistema in maniera pseudonima, in modo da consentire il record linkage impedendo nel contempo l'individuazione diretta della persona, tutelandone l'identità e garantendone la riservatezza;
   - caricamento sul sistema dei dati secondo i tracciati e le modalità previste dal sistema di stratificazione;
   - esecuzione della stratificazione della popolazione assistita e assegnazione alle classi indicate nel paragrafo dedicato alla stratificazione;
   - estrapolazione e utilizzo dei dati in forma aggregata, secondo classi predefinite o altre associazioni diagnostiche per creare macrogruppi utili all'attività previste dalla medicina di iniziativa.

3. I risultati del trattamento consistono in report/liste/schede riguardanti:
   - la qualità dei dati inseriti, completezza dei dati, validità codici diagnosi e farmaci, controlli logico-formali;
   - la prevalenza delle malattie con confronti standardizzati per età e sesso tra gruppi di popolazione;
   - la prevalenza delle categorie di comorbilità nella popolazione generale e indicatori di confronto per gruppi di popolazione;
   - gli indici di consumo di risorse osservati e aggiustati per case-mix nella popolazione generale e per gruppi di popolazione;
   - la previsione di costi per specifiche malattie o gruppi di case-mix;
   - l'aderenza alla terapia farmacologica;
   - gli elenchi di soggetti selezionabili in base ai valori assunti dagli indici di rischio o da qualunque altra variabile disponibile nell'archivio;
   - le informazioni individuali che rappresentano la sintesi delle principali informazioni cliniche e degli indicatori di rischio per singolo paziente.

4. Alla Provincia, nonché alle strutture e professionisti accreditati e convenzionati del servizio sanitario provinciale, per le finalità di cui al presente regolamento verranno trasmessi dati aggregati e anonimizzati secondo tecniche allo stato dell'arte di cui al disciplinare tecnico allegato, per le attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, di cui alla lettera v) del comma 2 art. 2 sexies del decreto legislativo 196/2003.

5. La comunicazione di dati personali alle strutture e professionisti accreditati e convenzionati del servizio sanitario provinciale (es. medici di medicina generale, pediatri di libera scelta, medici

specialisti) specificamente individuati nell'ambito della medicina di iniziativa e per finalità connesse a tale attività, potrà avvenire solo per finalità di tutela della salute degli interessati in carico a tali strutture e professionisti, e quindi solo previo consenso degli stessi, utilizzando le misure tecniche e di sicurezza individuate nel disciplinare tecnico allegato.

6. Le informazioni comunicate per la finalità di cui al punto 5 riguarderanno i pazienti in carico al clinico, il loro stato di salute, la/le condizione/i cronica/che e i fattori di rischio, l'appartenenza a classi diagnosi e gruppi di comorbilità, considerando anche la prognostica della patologia o condizione, il livello di utilizzazione di risorse, il rischio di ricovero/ospedalizzazione, l'appartenenza a gruppi di diagnosi farmaco-correlati.

Art. 8
Diffusione dei dati

1. Il Titolare del trattamento, per le finalità di cui all'articolo 3, può pubblicare dati adottando tecniche di anonimizzazione allo stato dell'arte.

Art. 9
Soggetti autorizzati e Responsabili del trattamento

1. I dati personali inerenti il trattamento di cui al presente regolamento sono trattati nel rispetto dei principi di cui all'articolo 5 del Regolamento (UE) 2016/679, in particolare liceità, correttezza, trasparenza, pertinenza e minimizzazione, soltanto da personale istruito dal Titolare del trattamento e che opera sotto la sua autorità, ai sensi dell'articolo 29 del Regolamento, e sottoposto a regole di condotta analoghe al segreto professionale stabilite dal Titolare del trattamento qualora non sia tenuto per legge al segreto professionale.
2. I dati potranno altresì essere trattati da soggetti terzi che svolgono per il Titolare delle attività strumentali al raggiungimento delle finalità del trattamento indicate all'art. 3, quale ad esempio il fornitore per le attività di assistenza sullo strumento informatico utilizzato per il trattamento.
3. I soggetti autorizzati e i Responsabili del trattamento accedono ai dati secondo modalità, strumenti, logiche di elaborazione e visibilità dei dati identificativi degli interessati strettamente pertinenti e non eccedenti ai compiti attribuiti a ciascuno di essi nel rispetto di quanto previsto nel disciplinare tecnico allegato.

Art. 10
Sicurezza dei dati personali

1. Il Titolare del trattamento dei dati adotta misure tecniche e organizzative individuate ai sensi degli articoli 25 e 32 del Regolamento (UE) 2016/679, anche a seguito di un'adeguata valutazione d'impatto sulla protezione dei dati condotta ai sensi dell'art. 35 del medesimo Regolamento e specificate nel disciplinare tecnico di cui all'allegato A al presente regolamento, che ne forma parte integrante.
2. In particolare, il trattamento delle particolari categorie di dati personali con l'ausilio di strumenti elettronici avviene mediante l'utilizzo di tecniche di pseudonimizzazione, anche con il ricorso a codici identificativi, nel rispetto di quanto previsto dal disciplinare tecnico di cui all'allegato A al presente regolamento, in modo tale da tutelare l'identità e la riservatezza degli interessati, rendendoli temporaneamente inintelligibili e permettendo di identificare gli interessati solo in caso di necessità o per finalità di cura, riabilitazione e prevenzione.

3. La scelta dell'algoritmo di stratificazione da utilizzare deve essere orientata agli standard de facto in ambito sanitario e scientifico per lo studio di queste tipologie di dataset, possedere elevati livelli di accuratezza e prevedere la trasformazione dal singolo dato clinico (diagnosi codificata) in gruppi di patologie correlate, di livello crescente di gravità e di complessità assistenziale.
4. Le particolari categorie di dati personali sono trattate con le modalità di cui al comma 2 anche quando il trattamento avviene senza l'ausilio di strumenti elettronici.
5. Le particolari categorie di dati personali sono trattate e conservate separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Art. 11
Informativa agli interessati

1. Il Titolare del trattamento dei dati deve fornire l'informativa agli interessati, nelle modalità previste dagli articoli 78 e 79 del D.Lgs 196/2013 e secondo le indicazioni contenute negli artt. 13 e 14 del Regolamento UE 2016/679, anche attraverso il proprio sito internet istituzionale, ai sensi dell'articolo 14, par. 5, lett. b) del Regolamento (UE) 2016/679.
2. Il Titolare del trattamento è tenuto a garantire agli interessati il pieno e tempestivo esercizio dei diritti previsti da tali articoli.

Art. 12
Conservazione dei dati

1. I dati personali verranno conservati per un periodo di 10 anni dalla loro raccolta, in conformità al principio di "limitazione della conservazione" di cui all'articolo 5, par. 1, lett. e), del Regolamento.

Art. 13
Norme transitorie

1. L'adeguamento e l'adozione delle modalità tecniche e delle misure di sicurezza di cui al disciplinare tecnico previsto dall'articolo 10, devono avvenire entro 180 giorni dall'entrata in vigore del presente regolamento.

Art. 14
Entrata in vigore

1. Ai sensi dell'art. 57 dello Statuto di autonomia, il presente regolamento entra in vigore il quindicesimo giorno successivo alla sua pubblicazione sul Bollettino Ufficiale della regione TAA.

Il presente decreto sarà pubblicato nel "Bollettino ufficiale" della Regione.
E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Elenco degli allegati parte integrante

001 Allegato

IL PRESIDENTE
Maurizio Fugatti

Allegato A)

DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA

Premessa

Il presente disciplinare tecnico specifica le misure tecniche e organizzative di cui agli articoli 25 e 32 del Regolamento (UE) 679/2016, da verificare periodicamente da parte del Titolare del trattamento, anche a seguito di una valutazione d'impatto sulla protezione dei dati effettuata ai sensi dell'articolo 35 del medesimo Regolamento.

Il presente disciplinare tecnico specifica in particolare:

A) le modalità tecniche delle operazioni di cui all'art. 7 del regolamento che possono avvenire mediante:

a) accesso diretto degli addetti a documenti, archivi, registri, flussi, database di cui all'articolo 6 del regolamento;

b) invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web (web service) o cooperazione applicativa);

c) trasmissione di documenti cartacei in plico chiuso e sigillato.

B) le misure di sicurezza che:

a) il Titolare del trattamento, il Responsabile e i soggetti autorizzati devono adottare per l'esecuzione delle operazioni sui dati di cui all'art. 7 del regolamento;

b) il Titolare del trattamento, il Responsabile e i soggetti autorizzati, presso i quali sono raccolti i dati di cui all'art. 5 del regolamento, devono adottare per comunicare o mettere a disposizione i dati al Titolare del trattamento.

DISPOSIZIONI GENERALI

Il Titolare e il Responsabile del trattamento istruiscono gli addetti, individuati ai sensi dell'art. 2-quaterdecies del decreto legislativo 30 giugno 2003, n. 196, sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina in materia di protezione dei dati personali più rilevanti in rapporto alle relative attività, nonché sulle responsabilità che ne derivano.

La sicurezza dei dati contenuti in documenti, archivi, registri, flussi e database deve essere garantita in tutte le fasi del trattamento, adottando opportuni accorgimenti tecnico-organizzativi che preservino i dati da 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. A tal fine si utilizzano tecniche di pseudonimizzazione e si garantisce, ove le finalità non richiedano il loro utilizzo, la separazione dei dati anagrafici da quelli sanitari.

Gli strumenti informatici utilizzati per il trattamento dei dati sono dotati di:

a) sistemi antivirus e antimalware costantemente aggiornati;

b) sistemi di protezione perimetrale, costantemente attivati e adeguatamente configurati in funzione del contesto operativo (firewall);

c) software di base e applicativo costantemente aggiornato.

MISURE DI SICUREZZA

1) Autorizzazione, abilitazione, autenticazione e tracciamento degli accessi

Le operazioni eseguibili di cui all'art. 7 del regolamento devono conformarsi alle seguenti modalità:

a) assegnare al personale addetto al trattamento credenziali di autenticazione e relativi livelli di autorizzazione

specifici alle attività di consultazione;

b) predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione del personale addetto al trattamento dei dati, nonché per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati garantendo che:
   - le operazioni sui dati avvengano soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP del Titolare del trattamento o dotate di certificato digitale, emesso da una Certification Authority ufficiale, che identifichi univocamente la postazione di lavoro;
   - laddove le operazioni sui dati avvengano secondo le modalità della cooperazione applicativa, in forma di web service, le condizioni d'uso di tali servizi, che devono individuare idonee garanzie per il trattamento dei dati personali, siano trasposte in appositi accordi di servizio, secondo le specifiche tecniche del Sistema pubblico di connettività (SPC) istituito dal Codice dell'Amministrazione Digitale;
   - laddove invece le operazioni sui dati avvengano attraverso l'utilizzo di applicazioni web su Internet, vengano impiegati protocolli di comunicazione protetti (protocolli https/ssl); siano visualizzabili le informazioni relative alla sessione corrente e all'ultima sessione effettuata con le stesse credenziali (con l'indicazione almeno di data, ora e indirizzo di rete da cui è effettuata la connessione); sia asseverata l'identità digitale dei server erogatori di servizi, tramite l'utilizzo di certificati digitali emessi da una Certification Authority iscritta all'elenco nazionale dei certificatori attivi;
   - nella fase transitoria di cui all'articolo 13 del regolamento, necessaria per l'adeguamento tecnologico, la password venga consegnata al singolo addetto separatamente rispetto al codice per l'identificazione e sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi; nella fase transitoria di cui all'art. 13, le credenziali assegnate agli utenti siano registrate sui sistemi AD / LDAP / Kerberos aziendali, le password siano quelle standard windows archiviate in HASH;
   - sia vietata la possibilità di effettuare accessi contemporanei allo stesso sistema con le medesime credenziali;
   - sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;
   - siano disattivate le credenziali di autenticazione non utilizzate da almeno sei mesi;
c) effettuare periodiche verifiche, anche a fronte di cambiamenti organizzativi o eventi anomali, circa la sussistenza dei presupposti che hanno originato l'abilitazione degli addetti. Eventuali esiti negativi delle predette verifiche, devono dar luogo alla tempestiva revisione dei livelli di abilitazione, all'eventuale disabilitazione dello stesso o alla disattivazione delle credenziali;
d) prevedere la registrazione in appositi file di log, ai fini della verifica della liceità del trattamento dei dati e di corretto accesso agli stessi, delle seguenti informazioni: il soggetto (codice identificativo) che ha effettuato l'accesso, la data e l'ora dell'accesso, l'operazione effettuata, l'indirizzo IP della postazione di lavoro e del server interconnesso, l'identificativo univoco del paziente (se presente) i cui dati sono stati elaborati. Inoltre:
   - i log sono protetti con idonee misure atte a garantire integrità e inalterabilità contro ogni uso improprio, tramite criptazione e logging degli accessi effettuati ai log;
   - i log sono conservati per almeno 24 mesi;
e) utilizzare sistemi di audit log per la verifica periodica degli accessi ai dati e per il rilevamento delle anomalie;
f) i log sono accessibili esclusivamente agli amministratori di sistema nominati dal Titolare, gli accessi degli amministratori sono loggati.

Per l'accesso al sistema, garantendo la segregation of duties SoD organizzativa, vengono definiti i seguenti profili distinti di autorizzazione:

a) profilo del personale (amministratore di sistema) che accede alle fonti dati e carica le informazioni nel sistema in forma pseudonima;
b) profilo del personale (gruppo tecnico di progetto) che accede ai dati del sistema in forma pseudonima per effettuare analisi di stratificazione;
c) profilo del personale (amministratore di sistema) che può effettuare la reidentificazione degli assistiti;

d) profilo del personale (gruppo tecnico di progetto, medici / operatori sanitari) che possono utilizzare i dati del sistema reidentificati per il reclutamento degli assistiti nell'ambito della medicina di iniziativa e per finalità connesse a tale attività; tale utilizzo potrà avvenire solo per finalità di tutela della salute degli interessati in carico a tali strutture e professionisti e, quindi, solo previo consenso.

I dati in formato aggregato o anonimizzato saranno resi disponibili alle articolazioni aziendali competenti per svolgere attività di governance (pianificazione, monitoraggio, verifica delle performance e del raggiungimento degli obiettivi).

2) Invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web (web service) o cooperazione applicativa)

Il Titolare comunica i dati nel rispetto di quanto previsto dal presente disciplinare tecnico e dal provvedimento del Garante per la protezione dei dati personali recante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche n. 393 del 2 luglio 2015".

L'invio telematico dei dati avviene adottando le seguenti misure di sicurezza:

a) utilizzo di canali di trasmissione protetti (FTP sicuro, VPN IPSEC/SSL o HTTPS o sistemi equivalenti) adeguati in relazione allo stato dell'arte dell'evoluzione tecnologica;

b) nel caso di utilizzo della PEC, è possibile inviare i dati sensibili o informazioni personali non come testo contenuto nell'oggetto o nel corpo del messaggio, ma solo se contenuti in file allegati cifrati o protetti con una chiave (ad es. con una password) comunicata disgiuntamente.

3) Accesso diretto degli addetti ai sistemi informatici

In generale i soggetti di cui all'art. 9 del regolamento accedono ai dati di cui all'articolo 5 del regolamento adottando le seguenti misure di sicurezza:

a) utilizzo di protocolli di comunicazione protetti (VPN, IPSEC/SSL o canali HTTPS) predisposti dal Titolare verso i soggetti autorizzati;

b) identificazione, autenticazione, autorizzazione degli addetti abilitati ad accedere ai dati di cui all'art. 5 del regolamento.

4) Trasmissione su supporti informatici (es. CD, DVD, memorie a stato solido)

I soggetti autorizzati alla raccolta delle informazioni di cui all'articolo 5 del regolamento, effettuata mediante trasmissione su supporti informatici, sono tenuti ad adottare le seguenti misure di sicurezza:

a) i supporti informatici devono essere inseriti in plico chiuso, inviati mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo;

b) devono essere utilizzati accorgimenti tecnici per garantire l'integrità dei dati contenuti in tali supporti.

5) Trasmissione di documenti cartacei

I soggetti autorizzati alla raccolta delle informazioni di cui all'articolo 5 del regolamento, effettuata mediante trasmissione di documenti cartacei, sono tenuti ad adottare le seguenti misure di sicurezza:

a) i documenti cartacei devono essere inseriti in plico chiuso, inviati mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo;

b) sul plico apporre la dicitura "Contiene dati personali. Riservato agli addetti del trattamento del Dipartimento interessato";

c) utilizzare plichi o "incarti" non trasparenti al fine di rendere inintelligibile il contenuto;

d) apporre una firma o sigla sui lembi di chiusura del plico.

È in ogni caso vietato inviare in chiaro via fax, via mail, via protocollo informatico, documenti contenenti dati personali e particolari.

6) Elaborazione dei dati

Ai fini dell'attuazione di quanto previsto all'articolo 7 del regolamento e prima di effettuare la stratificazione, ad ogni assistito viene assegnato un codice univoco pseudonimo volto a non consentire la identificazione diretta dell'interessato durante il trattamento dei dati; il codice consiste in una sequenza di lunghezza fissa di caratteri alfanumerici casuali.

Ad ogni assistito preso in carico da APSS, viene assegnato un codice univoco anagrafico, registrato sull'anagrafe unica centralizzata aziendale, che implementa un Master Patient Id (MPI), conforme al profilo PIX (Patient Information Cross Reference) dell'IT Infrastructure Technical Framework, emanato da Integrating the Healthcare Enterprise (IHE).

Quindi, al codice univoco anagrafico viene associato un codice univoco-criptato non invertibile utilizzando, in prima battuta, un algoritmo di HASH con algoritmo SHA-256; a regime, si utilizzerà un algoritmo HMAC-SHA-256 con digest di output codificato in Base64, con chiave protetta da apposite misure tecniche (chiave esterna ai sistemi) e accessibile solo a personale autorizzato.

Per la pseudonimizzazione si è preso a riferimento il documento ENISA "Tecniche di pseudonimizzazione e migliori pratiche - Raccomandazioni per sviluppare tecnologie conformi alle disposizioni in materia di protezione dei dati e privacy" novembre 2019, in particolare i paragrafi 5.1.3 Funzione crittografica di hash (HASH) e 5.1.4 Codice di autenticazione del messaggio (HMAC) e il "Parere 05/2014 sulle tecniche di anonimizzazione" del WP29 (Working Party doc 0829/14/IT WP216), paragrafo dedicato alla pseudonimizzazione.

Attraverso tale sistema di codifica non invertibile, i dati riferiti ad ogni singolo assistito continueranno ad essere riferibile ad un singolo individuo, sempre lo stesso, a prescindere dalla fonte informativa da cui proviene il dato, in modo da consentire il record linkage; tuttavia, non si potrà effettuare alcuna correlazione diretta tra tale codice univoco e i dati anagrafici dell'interessato e non sarà quindi possibile ricondurre i dati direttamente all'assistito.

La reidentificazione della persona potrà essere effettuata nei soli casi strettamente indispensabili nei quali, soltanto per specifiche esigenze di controllo e verifiche previste dalla normativa, il Titolare autorizzerà tale operazione. In tali casi, la riassegnazione ai dati identificativi della persona dei dati pseudonimizzati potrà avvenire riapplicando il processo di pseudonimizzazione e ricostruendo l'associazione codice univoco anagrafico – codice criptato, conservando per il solo tempo strettamente necessario all'operazione la mappatura codice univoco anagrafico – codice criptato.

La trasmissione di dati alla Provincia o la diffusione potrà avvenire o in forma aggregata oppure, a seguito dell'anonimizzazione degli stessi, attraverso l'applicazione ai dati personali di tecniche che consentano di ottenere la deidentificazione irreversibile degli stessi e, quindi, di ridurre al minimo il rischio anche potenziale di reidentificare il paziente c.d. "single-out".

Le tecniche utilizzate apparterranno alla famiglia della generalizzazione, secondo quanto indicato nel "Parere 05/2014 sulle tecniche di anonimizzazione" del WP29 (Working Party doc 0829/14/IT WP216), in particolare al par. 3.2.2. L-L-diversità/T-vicinanza; per WP29 tali tecniche presentano in generale basso rischio di reidentificazione e di deduzione, permanendo un qualche rischio di correlabilità / deduzione v. par. Raccomandazioni. Qualunque sia la tecnica adottata, sarà oggetto di periodica rivalutazione.

I dati sono trattati dagli addetti esclusivamente attraverso applicazioni software dotate di adeguati sistemi di autenticazione e di autorizzazione in funzione del ruolo degli addetti e delle esigenze di accesso e trattamento dei dati, avendo cura di delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati e di predisporre meccanismi per la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi. Tali applicazioni devono possedere le seguenti caratteristiche:

a) un sistema di autenticazione a più fattori. Nella fase transitoria di cui all'articolo 13 del regolamento, necessaria per l'adeguamento tecnologico a tale soluzione, non superiore a giorni 180 dall'entrata in vigore del regolamento, è possibile utilizzare credenziali costituite da codice identificativo e parola chiave riservata robusta, univoca, non condivisa, modificata con cadenza massima di 90 giorni;
b) sia vietata la possibilità di effettuare accessi contemporanei allo stesso sistema con le medesime credenziali;
c) sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;

d) siano visualizzabili le informazioni relative alla sessione corrente e all'ultima sessione effettuata con le stesse credenziali (con l'indicazione almeno di data, ora e indirizzo di rete da cui è effettuata la connessione).

Le postazioni di lavoro utilizzate per il trattamento dei dati devono appartenere alla rete IP del Titolare del trattamento o essere dotate di certificato digitale, emesso da una Certification Authority ufficiale, che identifichi univocamente la postazione di lavoro.

L'interconnessione tra dati informatizzati e dati su supporto cartaceo avviene in assenza di sistema di codifica. In tal caso il trattamento è effettuato esclusivamente da personale espressamente individuato dal Titolare, sottoposto a regole di condotta analoghe al segreto professionale stabilite dal Titolare del trattamento qualora non sia tenuto per legge al segreto professionale.

7) Conservazione dei dati e copie di sicurezza

I dati trattati dal Titolare del trattamento, vengono memorizzati e conservati in luoghi e con modalità prestabilite dal Titolare stesso, in modo tale da proteggere l'identità e tutelare la riservatezza degli interessati.

I dati sono conservati con garanzie di riservatezza, integrità e disponibilità.

I supporti informatici e i documenti cartacei devono essere riposti dagli addetti in appositi archivi, organizzati secondo una documentata procedura relativa alla nomenclatura e alla classificazione dei supporti in modo che siano univocamente identificabili, soltanto attraverso apposito codice in caso di necessità e di verifica.

Per quanto attiene le copie di sicurezza previste per il salvataggio dei dati e delle applicazioni, utili ai fini del recupero in caso di perdita accidentale o per altre cause, esse vengono predisposte ed eseguiti con sistemi e servizi di back-up in conformità a quanto previsto dalle politiche di backup del Titolare.

È compito del Titolare o di suo delegato implementare e presidiare quotidianamente la corretta applicazione delle politiche interne per le copie di sicurezza e l'esecuzione delle copie stesse, così come le azioni inerenti il ripristino dei dati.

Le copie di sicurezza vengono inviate secondo una periodicità prefissata ad un sito parallelo implementato presso l'ente strumentale provinciale di servizi ICT, che in quanto tale è identificato come Responsabile esterno di trattamento.

8) Accesso ai locali

L'accesso ai locali ove si svolge il trattamento dei dati, ivi compresi i locali destinati a ospitare gli archivi di supporti informatici o cartacei, deve avvenire secondo una documentata procedura, prestabilita dal Titolare del trattamento, che preveda l'identificazione delle persone che accedono e la registrazione degli orari di ingresso e uscita di tali persone.

9) Manutenzione dei sistemi informatici

I soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici, che possono comportare il trattamento dei dati, devono essere designati Responsabili del trattamento.

I contratti di manutenzione, stipulati con i predetti soggetti esterni, devono prevedere specifiche clausole di riservatezza dei dati, la registrazione degli interventi con l'indicazione degli orari di inizio e fine, le persone che li hanno effettuati e le motivazioni che hanno determinato la necessità dei medesimi interventi.

10) Cancellazione dei dati e dismissione dei supporti e documenti contenenti dati

I dati trattati per le attività di cui al presente regolamento devono essere cancellati o anonimizzati secondo tecniche allo stato dell'arte in maniera irreversibile trascorso un periodo di dieci anni dalla loro raccolta.

La procedura di anonimizzazione di cui al punto precedente adotta tecniche adeguate alla protezione dell'identità del paziente da rischi legati all'identificabilità mediante individuazione, correlabilità e deduzione a partire dai dati sanitari. Devono essere applicate tecniche di randomizzazione e generalizzazione dei dati, tenuto conto dell'evoluzione tecnologica, in modo da mantenere nel complesso la distribuzione degli elementi rilevanti per finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria.

I supporti informatici (es. memorie di massa dei server e delle postazioni di lavoro, etc.) utilizzati per il

trattamento dei dati devono essere dismessi secondo quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" (G.U. n. 287 del 9 dicembre 2008).

11) Misure organizzative

Il personale autorizzato al trattamento dei dati è adeguatamente formato e istruito a tenere comportamenti corretti, in particolare:

- le postazioni di lavoro assegnate dall'azienda all'utente devono essere utilizzate con cura per i soli scopi e trattamenti indicati dall'APSS;
- non lasciare la postazione di lavoro incustodita e con sessioni di lavoro attive; a tal fine sono operative policy di dominio sulle postazioni di lavoro aziendali che attivano lo screen saver e il blocco degli schermi dopo 3/5 minuti di inattività;
- alla fine della giornata lavorativa, tutti i computer devono essere spenti;
- sulle postazioni di lavoro non devono essere presenti dati personali; tali dati devono obbligatoriamente essere memorizzate nelle directory condivise appositamente create e disponibili sui sistemi centrali, accessibili con credenziali individuali e protetti da sistemi di backup, antivirus / antimalware, firewall;
- i documenti cartacei che contengano dati riferiti o riferibili alla persona e che non sono soggetti di specifica conservazione, dopo l'uso devono essere distrutti tramite una macchina distruggi documenti; invece, i documenti soggetti ad archiviazione devono essere trattati secondo le procedure aziendali di protocollazione, conservazione, archiviazione;
- vanno rispettate e attuate le politiche di clean-desk / scrivania pulita, in modo che tutti i documenti, lettere, raccoglitori, report, soprattutto se contenenti dati personali, siano a fine giornata rimossi dalla scrivania e riposti in cassetti o armadi chiusi a chiave;
- non lasciare incustodite, presso le fotocopiatrici, le stampe di documenti contenti dati personali e utilizzare per la stampa di documenti contenenti dati "sensibili" la modalità di stampa "privata" con codice personale;
- custodire con cura le credenziali di accesso agli applicativi (UserId e Password) che sono personali e riservati e come tali non posso essere ceduti ad altro operatore, e garantire la diligente custodia dei dispositivi informatici in proprio esclusivo uso e possesso;

I soggetti esterni che trattano dati per conto di APSS sono nominati Responsabili del trattamento e agli stessi vengono fornite le relative istruzioni, ai sensi di quanto previsto dall'art. 28 del Regolamento UE 2016/679.

12) Violazioni di dati personali

Il Titolare adotta misure tecniche e organizzative adeguate a rilevare tempestivamente eventuali violazioni dei dati personali e adempiere alle previsioni di cui agli articoli 33 e 34 del Regolamento UE 2016/679.