ASR ABRUZZO
AGENZIA SANITARIA REGIONALE

ALLEGATO A

DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FUNZIONAMENTO DEL REGISTRO DELLA FIBROMIALGIA.

PREMESSA

In ottemperanza alle disposizioni dell'articolo 32 del Regolamento (UE) 2016/679 "Sicurezza del trattamento", il presente Disciplinare specifica:

1. le modalità tecniche di raccolta dei dati del Registro regionale della fibromialgia, che avviene mediante accesso diretto degli autorizzati al trattamento del Registro Regionale della Fibromialgia ai sistemi informatici delle strutture sanitarie;
2. le misure di sicurezza che:
   - il Titolare del trattamento del Registro Regionale della Fibromialgia deve adottare nella tenuta e per il funzionamento del registro medesimo;
   - le Strutture presso le quali sono raccolti i dati che alimentano il Registro Regionale della Fibromialgia, quali le Aziende sanitarie locali, devono adottare per comunicare o mettere a disposizione i dati al Titolare del trattamento.

DISPOSIZIONI GENERALI

Il Titolare del trattamento del Registro Regionale della Fibromialgia istruisce gli autorizzati al trattamento 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 nel Registro Fibromialgia deve essere garantita in tutte le fasi del trattamento dei dati, adottando opportuni accorgimenti che preservino i medesimi dati da rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

1. FASE DI RACCOLTA DEI DATI

1.1. Raccolta

La raccolta dei dati nel Registro Regionale della Fibromialgia avviene mediante l'immissione degli stessi da parte dei professionisti di cui all'art. 6 del Regolamento recante norme per il funzionamento del Registro.

1.2. Inserimento diretto

I professionisti di cui all'art. 6 del Regolamento raccolgono direttamente i dati e li inseriscono nel Registro Regionale della Fibromialgia. Ciascun professionista sarà autorizzato a raccogliere i dati di cui all'art. 5 del Regolamento e a inserirli, una volta verificata la sua identità, nel Registro Regionale della Fibromialgia con le modalità definite dal Regolamento.

1.3. Sicurezza dei dati raccolti

La raccolta dei dati deve conformarsi alle seguenti modalità:

- assegnare al personale autorizzato all'inserimento dei dati credenziali di autenticazione a due fattori;
- predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione del personale autorizzato al trattamento dei dati nonché per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati garantendo che:

    a) per la raccolta dei dati, effettuata tramite applicazioni web accessibili su Internet, devono essere utilizzati esclusivamente canali di comunicazione cifrati mediante protocollo HTTPS basato su TLS (versione 1.2 o superiore); deve essere garantita l'autenticazione dei server applicativi tramite certificati digitali X.509 validi e non scaduti, rilasciati da Certification Authority riconosciute dai principali sistemi operativi e browser; devono inoltre essere implementati adeguati controlli per la gestione, il rinnovo e la revoca dei certificati, nonché per la prevenzione di accessi non autorizzati o attacchi di tipo man-in-the-middle.

    b) la password venga inviata al singolo autorizzato e, successivamente, modificata almeno ogni due mesi;

    c) siano utilizzati sistemi di autenticazione a più fattori per l'abilitazione degli autorizzati del registro all'accesso telematico del Registro stesso;

    d) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;

    e) sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;

    f) prevedere la registrazione in appositi file di log, ai fini della verifica della correttezza e legittimità del trattamento dei dati, 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, i dati trattati. Inoltre:

        - i log sono protetti con idonee misure contro ogni uso improprio;
        - i log sono conservati per 24 mesi e cancellati alla scadenza;
        - i dati contenuti nei log sono trattati da personale appositamente autorizzato e formato al trattamento esclusivamente in forma aggregata;
        - possono essere trattati in forma non aggregata unicamente laddove ciò risulti indispensabile ai fini della verifica della correttezza e legittimità delle singole operazioni effettuate;

    g) utilizzare sistemi di audit log per la verifica periodica degli accessi ai dati e per il rilevamento delle anomalie.

2. FASE DI ELABORAZIONE DEI DATI

2.1. I dati raccolti nel Registro regionale della Fibromialgia sono trattati dagli autorizzati del Registro esclusivamente attraverso applicazioni software dotate di adeguati sistemi di autenticazione e di autorizzazione in funzione del ruolo degli autorizzati 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.

2.2 Devono essere altresì adottate le misure di sicurezza e gli accorgimenti tecnici specificati nelle lettere g) e h) del punto 1.3 del presente disciplinare.

3. FASE DI CONSERVAZIONE DEI DATI

3.1 I dati raccolti dal Titolare del trattamento del Registro regionale della Fibromialgia, devono essere 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.

3.2 I dati di cui al punto 3.1 devono essere conservati con garanzie di riservatezza, integrità e disponibilità, con conseguente possibilità di ripristino dei dati stessi in caso di guasti e malfunzionamenti, per un periodo di 1 anno, al fine di eventuali successive verifiche ed integrazioni dei dati.

4. MANUTENZIONE DEI SISTEMI INFORMATICI

4.1. Nel rispetto di quanto prescritto dall'articolo 28 del RGPD, i soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici, che possono comportare il trattamento dei dati del Registro Fibromialgia, devono essere designati Responsabili del trattamento in outsourcing e devono dare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD e garantisca la tutela dei diritti dell'interessato.

4.2 I contratti di manutenzione, stipulati con i soggetti di cui al punto 5.1, devono prevedere requisiti minimi di sicurezza informatica, devono essere coerenti con il contesto di rischio e proporzionati alla natura dei trattamenti e dei servizi prestati, incluse clausole specifiche riguardanti la protezione dei dati personali.

Gli stessi, al fine di garantire un adeguato livello di sicurezza e di continuità operativa devono contemplare specifiche disposizioni in materia di protezione dei dati personali, tra cui:

a) obblighi di riservatezza e confidenzialità in capo al personale incaricato;

b) l'obbligo di registrazione e tracciabilità degli interventi effettuati sui sistemi informatici;

c) l'indicazione, per ciascun intervento, della data, dell'orario di inizio e fine, dei soggetti che lo hanno eseguito e delle motivazioni che ne hanno determinato la necessità.

Nel caso di subfornitori (sub-responsabili), il fornitore deve ottenere autorizzazione specifica o generale da parte dell'Amministrazione e garantire che gli stessi rispettino integralmente le suddette disposizioni contrattuali.

5. CANCELLAZIONE DEI DATI E DISMISSIONE DEI SUPPORTI E DOCUMENTI CONTENENTI DATI

5.1. I dati presenti sul sistema informatico del Registro Fibromialgia devono essere cancellati o resi anonimi in maniera irreversibile trascorso un periodo di 30 anni dal decesso dell'interessato cui i dati si riferiscono.

5.2 La procedura di anonimizzazione di cui al punto precedente deve adottare 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.