Allegato 1

DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FUNZIONAMENTO DEL REGISTRO TUMORI IN ATTUAZIONE DELLA LEGGE REGIONALE 10 APRILE 2012, N. 6 (OSSERVATORIO EPIDEMIOLOGICO REGIONALE. REGISTRI REGIONALI DELLE CAUSE DI MORTE E DI PATOLOGIA).

PREMESSA

In relazione alle misure di sicurezza, individuate dall'articolo 32 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 (RGPD), questo discipinare specifica:

1) le modalità tecniche di raccolta dei dati di cui all'articolo 5, comma 2, del regolamento regionale sul funzionamento del Registro tumori, d'ora in poi Regolamento, presso gli archivi individuati all'articolo 6 del medesimo regolamento, che può avvenire mediante:

a) invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web, c.d. web services, o cooperazione applicativa);

b) accesso diretto degli incaricati del Registro tumori ai sistemi informatici delle strutture sanitarie di cui all'articolo 6 del Regolamento;

c) trasmissione su supporti informatici (es. CD, DVD, memorie a stato solido);

d) trasmissione di documenti cartacei in plico chiuso e sigillato nelle more della messa a regime delle modalità di cui alle lettere a), b) e c).

I supporti di cui alla lettera c) e d) sono utilizzati esclusivamente per estrapolare i dati da inserire nel Registro tumori;

2) le misure di sicurezza che:

a) il Titolare del trattamento del Registro tumori deve adottare nella tenuta e per il funzionamento del registro medesimo;

b) le strutture presso le quali sono raccolti i dati che alimentano il Registro tumori, quali la Regione le aziende sanitarie territoriali e ospedaliere, gli istituti di ricovero e cura a carattere scientifico (IRCCS) nonché le strutture sanitarie private accreditate, devono adottare per comunicare o mettere a disposizione i dati al Titolare del trattamento.

DISPOSIZIONI GENERALI

Il Titolare del trattamento del Registro tumori istruisce gli incaricati, individuati ai sensi dell'articolo 2 quaterdecies del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento UE n. 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), 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 tumori 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. A tal fine si utilizzano tecniche crittografiche con chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati personali e si garantisce, ove le finalità non richiedano il loro utilizzo, la separazione dei dati anagrafici da quelli sanitari.

Le postazioni di lavoro informatiche utilizzate per il trattamento dei dati necessari per la tenuta e il funzionamento del Registro tumori, sono dotate 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.

1. FASE DI RACCOLTA DEI DATI

1.1 Il Titolare del trattamento del Registro tumori raccoglie con periodicità semestrale dall'archivio regionale delle schede di dimissioni ospedaliere (SDO) della Regione i dati necessari all'individuazione dei casi diagnosticati di tumore oppure, ove necessario, alla verifica dei dati già presenti nel Registro tumori. Verifica inoltre l'esattezza e l'aggiornamento dei dati anagrafici dei soggetti iscritti o da iscrivere nel Registro tumori mediante il raffronto con i dati contenuti nell'Anagrafe sanitaria regionale degli assistibili.
La raccolta dei dati presso le banche dati e gli archivi di cui all'articolo 6 del Regolamento deve in ogni caso conformarsi alle seguenti modalità:

a) garantire l'accesso selettivo ai soli dati di cui all'articolo 5 comma 2 del Regolamento;

b) assegnare al personale incaricato del trattamento credenziali di autenticazione e profili di autorizzazione specifici alle attività di consultazione e raffronto;

c) predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione del personale incaricato al trattamento dei dati nonché per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati garantendo che:

c.1) la raccolta dei dati avvengano soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP del Titolare del trattamento del Registro tumori o dotate di certificato digitale, emesso da una *Certification Authority* ufficiale, che identifichi univocamente la postazione di lavoro;

c.2) laddove la raccolta dei dati avvenga secondo le modalità della cooperazione applicativa, in forma di *web services*, 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 decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale);

c.3) laddove invece la raccolta dei dati avvenga attraverso l'utilizzo di applicazioni web su Internet, vengano impiegati canali di trasmissione 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;

c.4) siano utilizzati sistemi di autenticazione a più fattori per l'abilitazione degli incaricati del registro all'accesso telematico agli archivi delle strutture sanitarie individuate dall'articolo 6, comma 1, del Regolamento, per estrapolare i dati destinati ad alimentare e ad aggiornare il Registro stesso;

c.5) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;

c.6) sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;

c.7) siano disattivate le credenziali di autenticazione non utilizzate da almeno sei mesi;

d) effettuare periodiche verifiche, anche a fronte di cambiamenti organizzativi o eventi anomali, circa la sussistenza dei presupposti che hanno originato l'abilitazione degli incaricati. Eventuali esiti negativi delle predette verifiche, devono dar luogo alla tempestiva revisione del profilo di abilitazione, alla eventuale disabilitazione dello stesso o alla disattivazione delle credenziali;

e) 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 incaricato del 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.

Nel caso di cooperazione applicativa:

- sono conservati i file di *log* degli invii delle informazioni al registro;
- sono conservati i file di *log* delle ricevute del registro;

- a seguito dell'avvenuta ricezione delle ricevute il contenuto delle comunicazioni effettuate è eliminato;

f) utilizzare sistemi di *audit log* per la verifica periodica degli accessi a dati e per il rilevamento delle anomalie.

1.2. Invio telematico. L'invio telematico dei dati al Registro tumori da parte delle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate 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) cifratura dei dati mediante sistemi crittografici basati su protocolli a chiave asimmetrica, la cui componente pubblica è resa nota alle aziende sanitarie, agli istituti di ricovero e cura a carattere scientifico e alle strutture sanitarie private accreditate dal Titolare del trattamento del Registro tumori; la componente "privata" della chiave è conservata in un dispositivo sicuro (*smart card*), assegnato al titolare medesimo, unitamente al relativo P.I.N.;

c) nel caso di utilizzo della PEC, cifratura dei dati sensibili che devono essere riportati in appositi allegati utilizzando gli strumenti di cui al punto b).

Il Titolare del trattamento dei dati del Registro tumori è tenuto a stipulare previamente una convenzione (o altro atto bilaterale) con ciascuno dei soggetti di cui all'articolo 6 del regolamento, secondo uno schema tipo predisposto dalla Regione o Provincia autonoma, volta a definire le specifiche modalità tecniche di raccolta dei dati e le misure di sicurezza nel rispetto di quanto previsto dal presente disciplinare tecnico e dal provvedimento del Garante per la protezione dei dati personali del 2 luglio 2015, recante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche".

1.3 Accesso diretto degli incaricati del Registro Tumori ai sistemi informatici delle strutture sanitarie. Il Titolare del trattamento dei dati del Registro tumori, per la raccolta delle informazioni di cui all'articolo 5, comma 2, effettuata con modalità informatiche direttamente dai propri incaricati presso i sistemi informatici delle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate, è tenuto ad adottare le seguenti misure di sicurezza:

a) utilizzo di canali di trasmissione protetti (VPN IPSEC/SSL o canali HTTPS);

b) identificazione, autenticazione, autorizzazione degli incaricati del Registro tumori, abilitati ad accedere alle fonti di dati di cui all'articolo 6 del regolamento.

1.4 Trasmissione su supporti informatici. Il Titolare del trattamento dei dati del Registro tumori, per la raccolta delle informazioni di cui all'articolo 5, comma 2, effettuata mediante trasmissione su supporti informatici, è tenuto 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.

1.5 Trasmissione di documenti cartacei. Il Titolare del trattamento dei dati del Registro tumori, per la raccolta delle informazioni di cui all'articolo 5, comma 2, effettuata mediante trasmissione di documenti cartacei è tenuto 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 incaricati del trattamento dell'Osservatorio epidemiologico dell'Agenzia regionale sanitaria (ARS)";

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 vietato inviare via fax documenti dati oggetto di trattamento.

2. FASE DI ELABORAZIONE DEI DATI

2.1. Ai fini dell'attuazione di quanto previsto all'articolo 11 del Regolamento, il sistema di codifica dei dati identificativi degli interessati raccolti dal Registro tumori deve consistere in un numero predefinito di caratteri alfanumerici ottenuti attraverso procedure di cifratura invertibili, con algoritmo biunivoco e reversibile.
2.2. I dati raccolti nel Registro tumori sono trattati dagli incaricati del Registro tumori esclusivamente attraverso applicazioni *software* dotate di adeguati sistemi di autenticazione e di autorizzazione in funzione del ruolo degli incaricati 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;
b) sia vietata la possibilità di effettuare accessi contemporanei 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).

2.3 Le postazioni di lavoro utilizzate per il trattamento dei dati devono appartenere alla rete IP del Titolare del trattamento del Registro tumori o essere dotate di certificato digitale, emesso da una *Certification authority* ufficiale, che identifichi univocamente la postazione di lavoro.
2.4 Devono essere altresì adottate le misure di sicurezza e gli accorgimenti tecnici specificati nelle lettere d), e) e f) del punto 1.1 del presente disciplinare.

3. FASE DI CONSERVAZIONE DEI DATI

3.1 I dati raccolti dal Titolare del trattamento del Registro tumori, codificati ai sensi del punto 2.1, 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 e integrazione dei dati.
3.3 Il ripristino dei dati di cui al punto 3.1 deve avvenire secondo una documentata procedura di *restore*, prestabilita dal Titolare del trattamento.
3.4 I supporti informatici e i documenti cartacei contenenti i dati del registro devono essere riposti dagli incaricati 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.

4. ACCESSO AI LOCALI DEL REGISTRO TUMORI

4.1. L'accesso ai locali del Registro tumori, 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.

5. MANUTENZIONE DEI SISTEMI INFORMATICI

5.1. 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 tumori, devono essere designati Responsabili del trattamento in *outsourcing*.
5.2. I contratti di manutenzione, stipulati con i soggetti di cui al punto 5.1, 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.

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

6.1. I dati presenti nel sistema informatico del Registro tumori devono essere cancellati o resi anonimi in maniera irreversibile trascorso un periodo di 30 anni dal decesso dell'interessato cui i dati si riferiscono.
6.2 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 espressamente previsti dal Regolamento all'articolo 3 comma 1 lettera d).
6.3. I supporti informatici (es. memorie di massa dei *server* e delle postazioni di lavoro, supporti rimovibili) del Registro tumori 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).
6.4. I supporti cartacei del Registro tumori, contenenti dati sanitari, devono essere distrutti secondo una documentata procedura, prestabilita dal Titolare del trattamento, entro un periodo di 10 anni dal decesso dell'interessato, cui i dati si riferiscono.