



CONSIGLIO REGIONALE DEL VENETO

IX LEGISLATURA

ALLEGATO AL REGOLAMENTO REGIONALE RELATIVO A:

**NORME PER IL FUNZIONAMENTO DEL REGISTRO DEI TUMORI DEL
VENETO, ISTITUITO CON LEGGE REGIONALE 16 FEBBRAIO 2010, N. 11**

**ALLEGATI
A - B**

Allegato A (Articolo 9).

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

Premessa

Ferme restando le misure di sicurezza, individuate negli articoli da 31 a 36 del decreto legislativo 30 giugno 2003 n. 196 e nel disciplinare tecnico pubblicato in Allegato B a tale Decreto, il presente disciplinare dispone ulteriori misure di sicurezza che:

- a) il titolare del trattamento dei dati contenuti nel Registro tumori, deve adottare per il funzionamento del Registro tumori medesimo;
- b) i medici segnalanti e le strutture (Aziende ULSS, Aziende Ospedaliere, Istituti di Ricovero e Cura a Carattere Scientifico nonché strutture sanitarie private accreditate) che comunicano, rispettivamente, alle Aziende ULSS e al titolare di cui alla precedente lettera a), dati ed informazioni devono adottare nella fase della comunicazione dei predetti dati ed informazioni.

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.

Il titolare del trattamento dei dati contenuti nel Registro tumori, deve rendere edotti gli incaricati del trattamento, individuati ai sensi dell'articolo 30 del decreto legislativo 30 giugno 2003 n. 196, dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività nonché delle responsabilità che ne derivano.

Le postazioni di lavoro informatiche, utilizzate per i trattamenti dei dati presso il Registro tumori, devono essere dotati di:

- a) sistemi *antivirus* aggiornati con cadenza giornaliera;
- b) sistemi di protezione perimetrale, costantemente attivati e adeguatamente configurati in funzione del contesto operativo (*personal firewall*);
- c) sistemi contro i codici malevoli (*malware*);
- d) certificato digitale, emesso da una *Certification Authority* ufficiale, che identifichi univocamente la postazione di lavoro medesima.

1. FASE DI COMUNICAZIONE DEI DATI AL TITOLARE DEI DATI CONTENUTI NEL REGISTRO TUMORI

1.1. I medici segnalanti, nella fase di comunicazione dei dati, prevista all'articolo 6, comma 1, del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto, nel rispetto delle linee guida e delle istruzioni emanate dalla Giunta regionale del Veneto con propria deliberazione, indicanti anche le procedure di accreditamento, sono tenuti ad adottare le seguenti misure di sicurezza:

- a) utilizzo di canali di trasmissione protetti (VPN/IPSEC o SSL o sistemi equivalenti in relazione all'evoluzione tecnologica);
- b) sottoscrizione delle informazioni con firma digitale.

I canali di trasmissione protetti di cui alla precedente lettera a) e il protocollo per la sottoscrizione digitale di cui alla lettera b) saranno messi a disposizione dalla Regione del Veneto entro 180 giorni dall'emanazione delle linee guida ed istruzioni sopra citate.

1.2. Le Aziende ULSS nella fase di comunicazione dei dati prevista all'articolo 6, comma 2, del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto, nel rispetto delle linee guida e delle istruzioni emanate dalla Giunta regionale del Veneto con propria deliberazione, sono tenute ad adottare le seguenti misure di sicurezza:

- a) utilizzo di canali di trasmissione protetti (VPN/IPSEC o SSL o sistemi equivalenti in relazione all'evoluzione tecnologica);
- b) cifratura dei dati mediante sistemi crittografici basati su protocolli a chiave asimmetrica, la cui componente "pubblica" è resa nota alle suddette Aziende ULSS dal titolare del trattamento dei dati contenuti nel Registro tumori;
- c) conservazione dei file di *log* degli invii delle informazioni al Sistema Epidemiologico Regionale (SER) e conservazione dei file di *log* delle ricevute, inviate dal sistema informatico del SER;
- d) cancellazione del contenuto delle comunicazioni effettuate, a seguito dell'avvenuta ricezione delle ricevute di cui alla precedente lettera c).

1.3. Le Aziende ULSS, le Aziende Ospedaliere, le strutture sanitarie private accreditate e gli Istituti di Ricovero e Cura a Carattere Scientifico, nella comunicazione delle informazioni prevista all'articolo 6, comma 3, del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto, si conformano alle modalità di cui al precedente punto 1.2.. Nei casi di accesso telematico diretto a fonti informative che contengano i dati di cui all'articolo 5 comma 2, le Aziende ULSS, le Aziende Ospedaliere, le strutture sanitarie private accreditate e gli Istituti di Ricovero e Cura a Carattere Scientifico sono tenute a:

- a) stipulare previamente, fermo restando quanto previsto dagli articoli 50 e 58 del decreto legislativo 7 marzo 2005, n. 82 e sentito il Garante per la protezione dei dati personali ai sensi dell'articolo 154, comma 1, lettera g), una convenzione con il titolare del trattamento dei dati contenuti nel Registro tumori, volta a definire le esclusive finalità per le quali è consentito il trattamento dei dati, le modalità dello stesso, i vincoli per assicurarne la correttezza nonché, in particolare, il numero massimo degli incaricati abilitabili ad accedere. Nella convenzione dovrà essere disciplinata altresì la procedura da seguire per le autenticazioni e le autorizzazioni degli incaricati abilitabili ad accedere. Tale procedura deve prevedere verifiche a cura del titolare del Registro tumori, a cadenza almeno trimestrale, circa la sussistenza dei presupposti che hanno originato l'abilitazione degli incaricati nonché la comunicazione alle strutture di cui all'articolo 6, comma 3, del Regolamento di eventuali esiti negativi delle predette verifiche, affinché queste procedano alla tempestiva revisione del profilo di abilitazione o alla eventuale disabilitazione del profilo dei soggetti precedentemente abilitati;
- b) assicurare l'accesso selettivo ai soli dati di cui all'articolo 5, comma 2, del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto;
- c) predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione degli incaricati abilitati ad accedere ai dati suddetti nonché per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati, garantendo che:
 - c.1) gli accessi ai dati avvengano soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP del titolare del trattamento dei dati contenuti nel Registro tumori o dotate di certificazione digitale che identifichi univocamente la postazione di lavoro;
 - c.2) laddove l'accesso ai dati avvenga secondo le modalità della cooperazione applicativa, in forma di *web services*, le condizioni d'uso di tali servizi siano trasposte in appositi "*Accordi di servizio*", redatti secondo il modello della cooperazione applicativa impiegata all'interno del Sistema Pubblico di Connettività (SPC) istituito dal Codice dell'amministrazione digitale. Gli "*Accordi di servizio*" devono individuare idonee garanzie per il trattamento dei dati personali, prevedendo, in particolare, il tracciamento delle operazioni compiute in cooperazione applicativa, con l'identificazione del soggetto che accede ai dati, il *timestamp*, l'indirizzo IP di provenienza del soggetto e del *server* interconnesso, l'operazione effettuata e i dati trattati;
 - c.3) laddove, invece, l'accesso ai dati avvenga su rete pubblica (INTERNET), in forma di *web application*, l'applicazione sia implementata con protocolli *https/ssl* provvedendo ad asseverare l'identità digitale dei *server* erogatori dei servizi, tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* ufficiale, e prevedendo il tracciamento delle operazioni compiute, con

l'identificazione del soggetto che accede ai dati, il *timestamp*, l'indirizzo IP di provenienza del soggetto e del server interconnesso, l'operazione effettuata ed i dati trattati;

- c.4) i dati contenuti nei *log* di tracciamento delle operazioni compiute siano conservati per un periodo non superiore a tre mesi e possano essere trattati solo da appositi incaricati al trattamento esclusivamente in forma anonima mediante loro opportuna aggregazione. Tali dati possono essere trattati in forma non anonima unicamente laddove ciò risulti indispensabile al fine di verificare la correttezza e la legittimità delle singole interrogazioni effettuate;
- c.5) la *password* che consente l'accesso venga consegnata al singolo incaricato separatamente rispetto al codice per l'identificazione e sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi;
- c.6) sia possibile utilizzare sistemi di strong-authentication per l'abilitazione degli incaricati del Registro all'accesso telematico agli archivi delle strutture sanitarie, individuati dall'articolo 6, comma 3, del Regolamento, per estrapolare i dati destinati ad alimentare e ad aggiornare il Registro stesso;
- c.7) siano introdotti meccanismi volti ad assicurare che gli accessi avvengano esclusivamente nell'ambito di intervalli temporali o di data predeterminati, definiti sulla base delle esigenze lavorative del titolare del trattamento dei dati contenuti nel Registro tumori;
- c.8) laddove l'interrogazione dei dati richiamati alla predetta lettera a) avvenga su rete pubblica (*Internet*) e in forma di *web application*, nella prima schermata successiva al collegamento per l'interrogazione dei predetti dati, siano visualizzabili le informazioni relative all'ultima sessione effettuata con le stesse credenziali (almeno con l'indicazione di data, ora e indirizzo di rete da cui è stata effettuata la precedente connessione). Le stesse informazioni devono essere riportate anche relativamente alla sessione corrente;
- c.9) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;
- c.10) sia vietato l'utilizzo di dispositivi automatici (*robot*) che consentano di consultare i dati in forma massiva.

1.4. Nel caso previsto dal punto 1.2. lettera b), la componente "privata" della chiave asimmetrica utilizzata per la codifica delle informazioni, inviate al titolare del trattamento dei dati contenuti nel Registro tumori, è conservata in un dispositivo sicuro (*smart card*), assegnato dal titolare medesimo al referente aziendale ULSS di cui all'articolo 6 comma 2, del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto, unitamente al relativo

P.I.N. Code, secondo una documentata procedura che definisca anche soluzioni operative nel caso di prolungata assenza del soggetto predetto.

1.5. È vietato inviare dati sensibili mediante posta elettronica.

1.6. È in ogni caso vietato inviare via fax documenti contenenti dati sensibili.

1.7. La Regione del Veneto consente al titolare del trattamento dei dati contenuti nel Registro tumori di effettuare, ove necessario, l'accesso agli archivi di cui all'articolo 6, commi 4 e 5, del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto, utilizzando sistemi di autenticazione, autorizzazione (profilatura degli utenti) e canali di trasmissione protetti (VPN/IPSEC o SSL o sistemi equivalenti in relazione all'evoluzione tecnologica) per l'accesso agli archivi medesimi. Tutto il personale del Registro tumori, incaricato dei suddetti trattamenti, deve possedere credenziali e profilatura specifiche all'attività di raffronto ovvero di consultazione degli archivi medesimi.

2. FASE DI ELABORAZIONE DEI DATI CONTENUTI NEL REGISTRO TUMORI

2.1. Ai fini dell'attuazione di quanto previsto all'articolo 10 del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto, il sistema di codifica di tutti i dati memorizzati su *file/database* presso il Registro, deve consistere in un numero predefinito di caratteri alfanumerici ottenuti attraverso procedure di cifratura invertibili, con algoritmo biunivoco e reversibile.

2.2. I dati contenuti nel Registro tumori devono essere trattati dagli incaricati del Registro esclusivamente attraverso applicazioni software dotate di sistemi di autenticazione e di autorizzazione adeguati in funzione dei ruoli degli Incaricati e delle esigenze di accesso e trattamento dei dati. Tali sistemi devono possedere le seguenti caratteristiche:

- a) un sistema di "autenticazione forte" ("*strong authentication*"). Nella fase transitoria, necessaria per l'adeguamento tecnologico a tale soluzione, non superiore a centottanta giorni dall'entrata in vigore del Regolamento recante norme per il funzionamento del Registro dei tumori del Veneto, è possibile utilizzare un sistema di autenticazione con credenziali la cui componente riservata ("*password*") sia robusta, univoca, non condivisa, modificata con cadenza massima di novanta giorni;
- b) la disabilitazione del profilo degli incaricati in caso di mancata autenticazione di questi ultimi per un periodo superiore ai centottanta giorni;
- c) delle procedure per la verifica periodica della qualità e coerenza dei profili autorizzativi assegnati agli incaricati del trattamento;
- d) dei sistemi di *audit log* per la verifica periodica degli accessi ai dati e per il rilevamento di eventuali anomalie.

3. FASE DI CONSERVAZIONE DEI DATI DEL REGISTRO TUMORI

3.1. I dati ricevuti dal titolare del trattamento dei dati del Registro tumori, ai sensi dei punti 1.2 e 1.3, e codificati ai sensi dei punti 2.1. e 2.2., devono essere memorizzati e conservati in luoghi e con modalità prestabiliti dal titolare del trattamento dei dati del Registro tumori, in modo tale da tutelare l'identità e la riservatezza degli Interessati.

3.2. I dati di cui al punto 3.1. devono essere conservati con garanzie di riservatezza, integrità e disponibilità dei dati, con capacità di ripristino degli stessi in caso di guasti o malfunzionamenti, per il periodo di 10 anni, al fine di consentire eventuali successive verifiche od integrazioni 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.

4. ACCESSO FISICO AI LOCALI DEL REGISTRO TUMORI

4.1. L'accesso ai locali del Registro tumori deve avvenire secondo una documentata procedura, prestabilita dal titolare del trattamento dei dati contenuti nel Registro medesimo, che preveda l'identificazione delle persone che accedono e la tracciabilità degli orari di ingresso ed uscita.

5. MANUTENZIONE DEI SISTEMI INFORMATICI

5.1. Nel rispetto di quanto prescritto dall'articolo 29 del decreto legislativo 30 giugno 2003 n. 196, 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, anche in conformità a quanto stabilito nel punto 25 dell'Allegato B al decreto legislativo 30 giugno 2003 n. 196, specifiche clausole di riservatezza dei dati, la registrazione degli interventi con l'indicazione dell'orario di inizio e di fine degli interventi, 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 sul sistema informatico del Registro tumori devono essere anonimizzati nel sistema informatico medesimo, trascorso il periodo di 30 anni dal decesso dell'interessato cui i dati si riferiscono.

6.2. I supporti di memoria di massa dei *server* e delle postazioni di lavoro 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).

6.3. I supporti cartacei del Registro tumori, contenenti dati relativi alla salute, devono essere distrutti secondo una documentata procedura, prestabilita dal

titolare del trattamento dei dati, trascorso il periodo di 10 anni dal decesso dell'interessato cui i dati si riferiscono.

Allegato B (Articolo 6).

**SCHEMA RECANTE LE INFORMAZIONI CHE I MEDICI DEVONO
COMUNICARE ALL'AZIENDA ULSS NEL CUI TERRITORIO
OPERANO.**

Scheda di Rilevazione Iniziale Nuovi Casi di Neoplasia		
Assistito		
Codice Fiscale/codice Stranieri Temporaneamente Presenti/codice Europei Non Iscritti		
Cognome (ed eventuale Detto)	Nome	
Data di Nascita	Sesso: (barrare il dato corretto)	Maschile Femminile
Comune	Prov.	
Stato Estero di Nascita	Cittadinanza	
Az. ULSS di Appartenenza		
Patologia Oncologica		
Patologia Oncologica Rilevata		
Medico segnalante		
Dati Esordio Malattia		
Primo centro che ha effettuato la diagnosi		
Data Diagnosi	Data Esordio Neoplasia	

Fonte (barrare il dato corretto)	dati	Esordio:	Riferiti Paziente	dal Da Documentazione
Dati segnalante				
Centro che segnala				
Presidio che segnala				
Azienda che segnala				
Data segnalazione				

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

I dati personali che La riguardano, inseriti in questa Scheda relativa a Nuovi Casi di Neoplasia in Veneto, saranno comunicati, per il tramite di un referente aziendale dell'Azienda ULSS di appartenenza al titolare del Registro tumori, Azienda ULSS n. 4 "Alto Vicentino" – Sistema Epidemiologico Regionale (SER), presso il quale è istituito il Registro tumori del Veneto, istituito con legge regionale 16 febbraio 2010, n. 11.

I suoi dati verranno codificati e trattati in maniera rigorosamente riservata e saranno diffusi solo in forma anonima, ad esempio attraverso pubblicazioni scientifiche, statistiche e convegni scientifici.

I dati saranno utilizzati soltanto per scopi di ricerca scientifica e, in particolare, al fine di individuare i fattori di rischio e gli esiti degli interventi di diagnosi precoce nonché delle terapie e dei percorsi diagnostico-terapeutici.

I dati saranno trattati anche con modalità informatizzate, anche per quanto riguarda l'ambito di comunicazione degli stessi, nei limiti di quanto previsto dal Regolamento regionale del Veneto n. del, recante norme per il funzionamento del Registro dei tumori del Veneto.

La raccolta dei dati è obbligatoria ai sensi del predetto Regolamento regionale.

Lei potrà esercitare i diritti di cui all'articolo 7 del decreto legislativo 30 giugno 2003 n. 196 (ad es. accedere ai Suoi dati personali, integrarli, aggiornarli,

rettificarli, opporsi al loro trattamento per motivi legittimi, ecc.) rivolgendosi al titolare del trattamento, Azienda ULSS n. 4 – Sistema Epidemiologico Regionale (SER), presso:

Azienda ULSS n. 4 “Alto Vicentino” – SER

Via Rasa, 9

36016 Thiene (VI).