Allegato (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 31, 32, 33, 34, 35 e 36 del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), e nel disciplinare tecnico di cui all'Allegato B al decreto legislativo medesimo, il presente disciplinare specifica:

a) le modalità tecniche di trasmissione dei dati al registro tumori da parte dei soggetti individuati all'articolo 5 del presente regolamento, che può avvenire mediante:

1) l'invio telematico;

2) l'accesso diretto degli incaricati del registro tumori ai sistemi informatici delle strutture sanitarie di cui all'articolo 5 del regolamento;

3) la trasmissione su supporti informatici quali CD o DVD;

4) la trasmissione di documenti cartacei;

b) le misure di sicurezza che:

1) il titolare del trattamento del registro tumori deve adottare per il funzionamento del registro medesimo;

2) le strutture presso le quali sono raccolti i dati che alimentano il registro tumori, quali la Regione, gli enti del servizio sanitario regionale di cui all'articolo 2, comma 1, della legge regionale 20 giugno 2003, n. 13 (Riorganizzazione del servizio sanitario regionale), nonché le strutture sanitarie private accreditate, devono adottare per comunicare dati e informazioni al titolare di cui al punto 1).

Il titolare del trattamento dei dati del registro tumori istruisce gli incaricati, individuati ai sensi articolo 30 del d.lgs. 196/2003, circa i rischi che incombono sui dati, le misure disponibili per prevenire eventi dannosi, i profili della disciplina in materia di protezione dei dati personali più rilevanti in rapporto alle relative attività, nonché le responsabilità che ne derivano.

Le postazioni di lavoro informatiche del registro tumori sono dotate 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).

1. FASE DI RACCOLTA DEI DATI

1.1. Il titolare del trattamento del registro tumori raccoglie dall'archivio regionale delle schede di dimissioni ospedaliere (SDO) della Regione, con periodicità semestrale, i dati necessari all'individuazione dei casi diagnosticati di tumore oppure, ove necessario, alla verifica dei dati già presenti nel registro. Effettua inoltre il raffronto con i dati contenuti nel *data base* dell'anagrafe degli assistibili. La raccolta avviene utilizzando sistemi di autenticazione e autorizzazione e canali di trasmissione protetti (VPN IPSEC/SSL o HTTPS o sistemi equivalenti in relazione all'evoluzione tecnologica). Gli incaricati del registro tumori addetti ai trattamenti devono possedere credenziali di autenticazione e profili di autorizzazione adeguati a tali specifiche attività di consultazione e raffronto.

1.2 L'invio telematico dei dati al registro tumori da parte enti del servizio sanitario regionale e delle strutture sanitarie accreditate avviene adottando le seguenti misure di sicurezza:

a) utilizzo di canali di trasmissione protetti (VPN IPSEC/SSL o canali HTTPS), adeguati 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 agli enti del servizio sanitario regionale e alle strutture sanitarie accreditate dal titolare del trattamento del registro tumori;

c) utilizzo di posta elettronica certificata con cifratura delle informazioni sensibili mediante gli strumenti di cui alla lettera b);

d) in alternativa a quanto previsto alla lettera a) e nel rispetto di quanto previsto alla lettera b), trasmissione su supporti informatici quali CD o DVD, non riscrivibili, inseriti in plico chiuso, mediante

corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo;

1.3 Il titolare del trattamento dei dati del registro tumori, per la raccolta delle informazioni di cui all'articolo 4, comma 2, effettuata con modalità informatiche direttamente dai propri incaricati presso i sistemi informatici degli enti del servizio sanitario regionale e delle strutture sanitarie 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 5 del presente regolamento.

Il titolare del trattamento dei dati del registro tumori è inoltre tenuto a:

a) stipulare previamente, fermo restando quanto previsto dagli articoli 50 e 58 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), e sentito il Garante per la protezione dei dati personali ai sensi dell'articolo 154, comma 1, lettera g), del d.lgs. 196/2003, una convenzione con i soggetti di cui all'articolo 5 del presente regolamento, 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 il numero massimo degli incaricati abilitati ad accedere. Nella convenzione deve essere disciplinata altresì la procedura da seguire per le autenticazioni e le autorizzazioni degli incaricati abilitati ad accedere. Tale procedura deve prevedere verifiche a cura del titolare del trattamento del registro tumori, a cadenza almeno trimestrale, circa la sussistenza dei presupposti che hanno originato l'abilitazione degli incaricati, nonché la comunicazione ai soggetti di cui all'articolo 5 del presente regolamento di eventuali esiti negativi delle predette verifiche, affinchè queste procedano alla tempestiva revisione del profilo di abilitazione o alla eventuale disabilitazione del profilo dei soggetti precedentemente abilitati
b) garantire l'accesso selettivo ai soli dati di cui all'articolo 4, comma 2, del regolamento;
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:
    1) gli accessi ai dati avvengano soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP del titolare del trattamento del registro tumori;
    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) istituita 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;
    3) laddove l'accesso ai dati avvenga su rete pubblica (Internet) in forma di web application, l'applicazione sia implementata con protocolli HTTPS/SSL, utilizzando un certificato SSL emesso dalla Certification Authority CA Regione Marche mentre l'identificazione del soggetto che accede ai dati avviene attraverso le modalità previste dall'articolo 64 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale);
    4) i dati contenuti nel log di tracciamento delle operazioni compiute siano conservati per un periodo di 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 legittimità e la correttezza delle singole interrogazioni effettuate;
    5) nella fase transitoria necessaria per l'adeguamento tecnologico, 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;
    6) sia possibile utilizzare sistemi di strong-authentication per l'abilitazione degli incaricati del registro

all’accesso telematico agli archivi delle strutture sanitarie individuate dall’articolo 5, comma 2, del presente regolamento, per estrapolare i dati destinati ad alimentare e ad aggiornare il registro stesso;

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 del registro tumori;
8) laddove l’interrogazione dei dati richiamati al punto 1 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;
9) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;
10) sia vietato l’utilizzo di dispositivi automatici 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 del registro tumori, è conservata in un dispositivo sicuro (smart card), assegnato al Titolare medesimo, unitamente al relativo PIN.
1.5 E’ in ogni caso vietato inviare via fax documenti contenenti dati sensibili.
1.6 La comunicazione dei dati contenuti su supporti cartacei da parte enti del servizio sanitario regionale e delle strutture sanitarie private accreditate può avvenire mediante invio di documenti cartacei inseriti in plico chiuso, mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo.

2. FASE DI ELABORAZIONE DEI DATI
2.1. Ai fini dell’attuazione di quanto previsto all’articolo 10 del regolamento, il sistema di codifica di tutti i dati memorizzati su file/database presso il 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 di cui al punto 2.1. 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. Tali applicazioni devono possedere le seguenti caratteristiche:
a) un sistema di autenticazione forte (strong authentication). Nel periodo transitorio di cui all’articolo 11 del presente regolamento 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 automatica del profilo degli incaricati in caso di non utilizzo per un periodo superiore a centoottanta giorni;
c) sistemi di audit log per la verifica periodica degli accessi ai dati e per il rilevamento delle anomalie.
Deve essere prevista inoltre una procedura per la verifica periodica della qualità e coerenza dei profili autorizzativi assegnati agli incaricati del trattamento.
2.3 I supporti informatici di cui alla lettera d) del punto 1.2 sono utilizzati esclusivamente per estrapolare i dati da inserire nel sistema informatico del registro tumori per la loro successiva elaborazione.
2.4 I supporti informatici e i documenti cartacei contenenti i dati 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 .

3. FASE DI CONSERVAZIONE DEI DATI
3.1 I dati raccolti dal titolare del trattamento del registro tumori, codificati ai sensi dei punti 2.1 e 2.2, devono essere memorizzati e conservati in luoghi e con modalità prestabilite dal titolare stesso, 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, con conseguente possibilità di ripristino in caso di guasti e malfunzionamenti, per un periodo di almeno trenta anni, al fine di eventuali successive verifiche e integrazioni.
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 AI LOCALI
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 tracciabilità degli orari di ingresso ed uscita.

5. MANUTENZIONDE DEI SISTEMI INFORMATICI
5.1. Nel rispetto di quanto prescritto dall'articolo 29 del d.lgs. 196/2003, i soggetti esterni che effettuano 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, in conformità a quanto stabilito dal punto 25 dell'Allegato B del d.lgs. 196/2003, 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 sul sistema informatico del registro tumori devono essere anonimizzati nel sistema informatico medesimo, trascorso un periodo di almeno trenta 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, concernente "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali", pubblicato nella G.U. n. 287 del 9 dicembre 2008.
6.3. I supporti cartacei del registro tumori, contenenti dati sanitari, devono essere distrutti secondo una documentata procedura, prestabilita dal titolare del trattamento, entro dieci anni dal decesso del soggetto cui i dati si riferiscono.