Allegato A

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 d.lgs. 196/2003 e nel disciplinare tecnico pubblicato nell'allegato B del citato d.lgs., il presente Disciplinare specifica:
A) le modalità tecniche di trasmissione dei dati concernenti il registro tumori da parte degli organismi di cui all'articolo 5 del regolamento, che può avvenire mediante:

1) invio telematico, anche mediante file transfer, servizi web (web services);
2) l'accesso selettivo, vigilato e controllato degli incaricati del registro tumori;
3) trasmissione su supporti informatici quali CD, DVD, memorie a stato solido;
4) trasmissione di documenti cartacei in busta chiusa e sigillata, nelle more della messa a regime delle modalità digitali descritte al numero 1).

B) le misure di sicurezza che:

1) il Titolare del trattamento dati del Registro Tumori Regionale 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 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 dati e informazioni al Titolare di cui al numero 1).

1. DISPOSIZIONI GENERALI

a. Il titolare ed i responsabili del trattamento dei dati contenuti nel Registro tumori istruiscono gli incaricati del trattamento, individuati ai sensi dell'articolo 30 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 sulla protezione dei dati personali più rilevanti in rapporto alle relative attività nonché sulle responsabilità che ne derivano.

b. Le postazioni di lavoro informatiche, utilizzate per i trattamenti dei dati presso il Registro tumori, devono essere dotate di:
   a) sistemi antivirus e antimalware costantemente aggiornati;
   b) sistemi di protezione perimetrale, costantemente attivati e adeguatamente configurati in funzione del contesto operativo;
   c) software di base costantemente aggiornato al fine di prevenire vulnerabilità.

c. Il Titolare del trattamento dei dati del Registro Tumori è inoltre tenuto a:
   a) garantire l'accesso selettivo ai dati provenienti dai flussi informativi di cui all'articolo 7 del regolamento;
   b) 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:

b1) gli accessi ai dati siano tracciabili, riconducibili a chi li ha effettuati e sia possibile risalire alla data ed all'ora dell'accesso;
b2) i dati contenuti nel log di tracciamento delle operazioni compiute siano conservati per un periodo non superiore a 24 mesi e siano 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 operazioni di trattamento dei dati effettuate;
b3) siano rispettate, da parte delle unità funzionali di cui all'articolo 5, comma 2, del regolamento, le disposizioni riportate nel presente disciplinare;
b4) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;
b5) laddove l'accesso ai dati avvenga su rete pubblica (Internet) in forma di web:

- l'applicazione sia implementata con protocolli https/ssl provvedendo ad asseverare 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;
- l'applicazione preveda il tracciamento delle operazioni compiute, con la registrazione del codice identificativo del soggetto che accede ai dati, il time-stamp, l'indirizzo IP di provenienza del soggetto e del server interconnesso, l'operazione effettuata e i dati trattati;
- l'applicazione preveda nella prima schermata, successiva al collegamento per l'interrogazione dei predetti dati, che siano visualizzabili le informazioni relative all'ultima sessione effettuata con le stesse credenziali, riportandone data, ora e indirizzo di rete.

d. E' in ogni caso vietato inviare via fax documenti contenenti dati sensibili.

2. FASE DI RACCOLTA DEI DATI

a. Entro sei mesi dal consolidamento delle informazioni provenienti dai flussi informativi di cui all'articolo 7, comma 3, lettera a), del regolamento, il DEP Lazio estrae i dati necessari all'individuazione dei nuovi casi diagnosticati di tumore per l'anno di rilevazione e li rende disponibili a ciascuna UF attraverso la piattaforma web centralizzata, relativamente ai casi residenti nella specifica area di competenza ai sensi dell'articolo 5, comma 2, del regolamento.

La messa a disposizione dei dati tra il DEP Lazio e le UF 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).

b. Le singole UF provvedono, quindi, all'aggiornamento, alla codifica e alla verifica della storia clinica dei casi di competenza. Le UF aggiornano il dato sulla definizione della patologia tumorale con informazioni relative a anamnesi, diagnosi e risultati di indagini clinico - strumentali, attraverso le fonti informative riportate all'articolo 7, comma 3, lettera b), del regolamento. Le UF inseriscono attraverso la piattaforma web centralizzata,

gli eventuali casi sfuggiti alla rilevazione effettuata utilizzando gli archivi regionali centralizzati.

c. Una volta a regime, le UF effettuano le operazioni di cui al punto 2.b entro un anno dal caricamento del dato sulla piattaforma web centralizzata da parte del DEP Lazio.

d. La trasmissione alle UF delle informazioni in possesso delle aziende sanitarie, delle strutture sanitarie accreditate e degli IRCCS e/o l'accesso alle medesime da parte delle UF, avviene nel rispetto di quanto previsto nel presente disciplinare.

e. Ogni anno, entro sei mesi dal consolidamento dei dati da parte delle UF, il DEP Lazio provvede alla verifica dei dati inseriti nella piattaforma web centralizzata e quindi al rilascio della casistica regionale. Il rilascio della casistica regionale da parte del DEP Lazio avviene nel rispetto delle cautele previste dall'articolo 12 del regolamento.

3. FASE DI ELABORAZIONE DEI DATI

a. Ai fini dell'attuazione di quanto previsto all'articolo 9 del regolamento, il sistema di codifica dei dati identificativi dei soggetti memorizzati sulla piattaforma web centralizzata presso il registro tumori deve consistere in un numero predefinito di caratteri alfanumerici ottenuti attraverso procedure di cifratura invertibili, con algoritmo biunivoco e reversibile.

b. I dati di cui al punto 3.a. 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. Tali applicazioni devono possedere le seguenti caratteristiche:
   a) un sistema di autenticazione a più fattori con credenziali la cui componente riservata (password) sia robusta, univoca, non condivisa, modificata con cadenza massima di novanta giorni e su connessione criptata;
   b) la disabilitazione automatica del profilo degli incaricati in caso di non utilizzo per un periodo superiore a centottanta giorni, nel rispetto di quanto previsto ai punti 7 e 8 dell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza) al d.lgs. 196/2003;
   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, anche in presenza di cambiamenti organizzativi o eventi anomali riguardanti la sussistenza di presupposti che hanno originato l'abilitazione degli incaricati.

c. 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.

4. FASE DI CONSERVAZIONE DEI DATI

a. I dati raccolti dal titolare del trattamento del registro tumori, codificati ai sensi del punto 3.a, 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 nonché garantire l'identificazione del personale che accede ai suddetti locali e la registrazione dei relativi orari di ingresso ed uscita.

b. I dati di cui al punto 4.a devono essere conservati con garanzie di riservatezza, integrità e disponibilità, con conseguente possibilità di ripristino dei dati stessi in caso di guasti e malfunzionamenti. Si adottano procedure di backup dei dati con frequenza giornaliera in orario notturno, consolidati settimanalmente e conservati in file annuali per un periodo di 1 anno, al fine di eventuali successive verifiche ed integrazione.

c. Il ripristino dei dati di cui al punto 3.a deve avvenire secondo una documentata procedura di restore, prestabilita dal Titolare del trattamento.

5. MANUTENZIONE DEI SISTEMI INFORMATICI

a. Nel rispetto di quanto prescritto dall'articolo 29 del d.lgs. 196/2003, i soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici possono essere designati Responsabili del trattamento in outsourcing.

b. I contratti di manutenzione, stipulati con i soggetti di cui al punto 5.a, devono contenere specifiche clausole che prevedano l'adozione delle disposizioni contenute nel disciplinare tecnico di cui all'allegato B del d.lgs. 196/2003, ai sensi del punto 25 del medesimo allegato.

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

a. I dati presenti sul sistema informatico del Registro Tumori devono essere anonimizzati nel sistema informatico medesimo dopo 30 anni dal decesso dell'interessato cui i dati si riferiscono.

b. I supporti di memoria di massa dei server e delle postazioni di lavoro del Registro Tumori, nonché gli altri supporti che contengono dati personali inerenti il registro tumori devono essere dismessi o distrutti secondo quanto previsto rispettivamente dagli allegati A e B del 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).

c. I supporti cartacei ed informatici 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.

Allegato B

DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FUNZIONAMENTO DEL REGISTRO DEI REFERTI DEI SERVIZI DI ANATOMIA PATOLOGICA (RSAP).

PREMESSA

Ferme restando le misure di sicurezza, individuate negli articoli da 31 a 36 d.lgs. 196/2003 e nel disciplinare tecnico pubblicato nell'allegato B del citato d.lgs., il presente Disciplinare specifica:
A) le modalità tecniche di trasmissione dei dati concernenti il RSAP da parte dei servizi di anatomia patologica mediante supporti informatici quali CD, DVD, memorie a stato solido;
B) le misure di sicurezza che:

1) il Titolare del trattamento dati del RSAP deve adottare per il funzionamento del registro medesimo;
2) i servizi di anatomia patologica presso i quali sono raccolti i dati che alimentano il RSAP devono adottare per comunicare dati e informazioni al Titolare di cui al punto 1).

1. DISPOSIZIONI GENERALI

1.1. Il titolare ed i responsabili del trattamento dei dati contenuti nel RSAP istruiscono gli incaricati del trattamento, individuati ai sensi dell'articolo 30 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 sulla protezione dei dati personali più rilevanti in rapporto alle relative attività nonché sulle responsabilità che ne derivano.

1.2. Le postazioni di lavoro informatiche, utilizzate per i trattamenti dei dati presso il DEP Lazio, devono essere dotate di:

a) sistemi antivirus e antimalware costantemente aggiornati;
b) sistemi di protezione perimetrale, costantemente attivati e adeguatamente configurati in funzione del contesto operativo;
c) software di base costantemente aggiornato al fine di prevenire vulnerabilità.

1.3. Il Titolare del trattamento dei dati del RSAP è inoltre tenuto a:

a) garantire l'accesso selettivo ai dati provenienti dai servizi di anatomia patologica di cui all'articolo 11 del regolamento;
b) predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione del personale incaricato al trattamento dei dati nonché per delimitare nel tempo la possibilità di accesso ai medesimi dati, garantendo che:

b1) gli accessi ai dati siano tracciabili, riconducibili a chi li ha effettuati e sia possibile risalire alla data ed all'ora dell'accesso;
b2) i dati contenuti nel log di tracciamento delle operazioni compiute siano conservati per un periodo non superiore a 24 mesi e siano 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 operazioni di trattamento dei dati effettuate;
b3) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali.

1.4. E' in ogni caso vietato inviare via fax documenti contenenti dati sensibili.

2. FASE DI RACCOLTA DEI DATI

Ai fini dell'attuazione di quanto previsto all'articolo 11 del regolamento, il DEP Lazio raccoglie i dati provenienti dai servizi di anatomia patologica con cadenza annuale.

La messa a disposizione dei dati tra il DEP Lazio e i servizi di anatomia patologica 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).

La trasmissione delle informazioni in possesso dei servizi di anatomia patologica avviene nel rispetto di quanto previsto nel presente disciplinare.

3. FASE DI ELABORAZIONE DEI DATI

3.1. Ai fini dell'attuazione di quanto previsto all'articolo 11 del regolamento, il sistema di codifica dei dati identificativi dei soggetti memorizzati presso il RSAP deve consistere in un numero predefinito di caratteri alfanumerici ottenuti attraverso procedure di cifratura invertibili, con algoritmo biunivoco e reversibile.

3.2. I dati di cui al punto 3.1. sono trattati dagli incaricati del DEP Lazio 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. Tali applicazioni devono possedere le seguenti caratteristiche:

a) un sistema di autenticazione a più fattori con credenziali la cui componente riservata (password) sia robusta, univoca, non condivisa, modificata con cadenza massima di novanta giorni e su connessione criptata;
b) la disabilitazione automatica del profilo degli incaricati in caso di non utilizzo per un periodo superiore a centottanta giorni, nel rispetto di quanto previsto ai punti 7 e 8 dell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza) al d.lgs. 196/2003;
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, anche in presenza di cambiamenti organizzativi o eventi anomali riguardanti la sussistenza di presupposti che hanno originato l'abilitazione degli incaricati.

3.3. 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.

4. FASE DI CONSERVAZIONE DEI DATI

4.1. I dati raccolti dal titolare del trattamento del RSAP, codificati ai sensi del punto 3.1, 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 nonché garantire l'identificazione del personale che accede ai suddetti locali e la registrazione dei relativi orari di ingresso ed uscita.

4.2. I dati di cui al punto 4.1 devono essere conservati con garanzie di riservatezza, integrità e disponibilità, con conseguente possibilità di ripristino dei dati stessi in caso di guasti e malfunzionamenti. Si adottano procedure di backup dei dati con frequenza giornaliera in orario notturno, consolidati settimanalmente e conservati in file annuali per un periodo di 1 anno, al fine di eventuali successive verifiche ed integrazione.

4.3. Il ripristino dei dati di cui al punto 3.1 deve avvenire secondo una documentata procedura di restore, prestabilita dal Titolare del trattamento.

5. MANUTENZIONE DEI SISTEMI INFORMATICI

5.1. Nel rispetto di quanto prescritto dall'articolo 29 del d.lgs. 196/2003, i soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici possono essere designati Responsabili del trattamento in outsourcing.

5.2. I contratti di manutenzione, stipulati con i soggetti di cui al punto 5.1, devono contenere specifiche clausole che prevedano l'adozione delle disposizioni contenute nel disciplinare tecnico di cui all'allegato B del d.lgs. 196/2003, ai sensi del punto 25 del medesimo allegato.

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

6.1. I dati presenti sul sistema informatico del RSAP devono essere anonimizzati nel sistema informatico medesimo dopo 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 RSAP, nonché gli altri supporti che contengono dati personali inerenti il RSAP devono essere dismessi o distrutti secondo quanto previsto rispettivamente dagli allegati A e B del 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 ed informatici del RSAP, 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.