OGGETTO: REGOLAMENTO PER IL FUNZIONAMENTO DEL REGISTRO TUMORI DELLA REGIONE TOSCANA

Sommario

PREAMBOLO

La Giunta regionale

Visto l'articolo 117, comma sesto, della Costituzione;

Visto l'articolo 42 dello Statuto;

Visto il 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Visto il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali);

Visto il decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale);

Visto il decreto legislativo 10 agosto 2018, n. 101 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Vista la legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale) ed, in particolare, l'articolo 20 ter;

Vista la legge regionale 3 aprile 2006, n. 13 (Trattamento dei dati sensibili e giudiziari da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo) e, in particolare, l'articolo 1, comma 1;

Visto il parere del Comitato di direzione espresso nella seduta del 25 luglio 2019;

Visto il parere della competente struttura di cui all'articolo 17, commi 4 e 5, del Regolamento interno della Giunta regionale Toscana 19 luglio 2016, n. 5

Vista la preliminare deliberazione di adozione dello schema di regolamento 5 agosto 2019, n.1060 (Regolamento per il funzionamento del registro tumori della Regione Toscana di cui all'articolo 20 ter della L.r. 40/2005);

Visto il parere favorevole della commissione consiliare competente, espresso nella seduta del 26 settembre 2019;

Visto l'ulteriore parere della competente struttura di cui all'articolo 17, commi 4 e 5, del Regolamento interno della Giunta regionale Toscana 19 luglio 2016, n. 5.

Considerato quanto segue:

1. L'articolo 2 sexies del d.lgs 196/2003 prevede che i trattamenti di categorie particolari di dati personali, necessari per motivi di interesse pubblico, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
2. L'articolo 20 ter della l.r. 40/2005, che ha istituito il registro tumori, prevede che debba essere adottato un regolamento regionale con cui disciplinare il trattamento dei dati personali ed, in particolare, dei dati relativi alla salute necessari alla tenuta del registro tumori;
4. Le Regioni hanno espresso la volontà di conformare i predetti trattamenti di dati personali alla disciplina in materia di protezione dei dati personali e, a tal fine, hanno ritenuto di condividere uno schema tipo per l'adozione del regolamento recante norme per il funzionamento del registro tumori e contenente, in allegato, un disciplinare tecnico in materia di misure di sicurezza, approvati dalla Conferenza delle Regioni e delle Provincie autonome il 15 febbraio 2018 (18/22/CR6a/C7) e trasmessi al Garante per la protezione dei dati personali in data 22 febbraio 2018;
5. Il Garante per la protezione dei dati personali ha collaborato con la Conferenza, fornendo tutte le indicazioni necessarie per la corretta impostazione dello schema di regolamento, ed ha espresso parere favorevole con provvedimento 227 del 18 aprile 2018;
6. Il Garante ha, altresì, precisato che l'adozione da parte delle regioni di un regolamento conforme allo schema tipo valutato positivamente non rende necessario chiedere all'autorità specifico parere.
Diversamente, qualora si intendano apportare modifiche sostanziali o integrazioni non formali riguardanti il trattamento dei dati personali rispetto allo schema tipo, occorrerà richiedere uno specifico parere su tali modifiche o integrazioni al Garante;
7. Essendo il presente regolamento conforme al predetto schema tipo, non si ritiene necessario sottoporlo ad ulteriore parere del Garante.

Approva il presente regolamento

Art. 1

Definizioni

1. Ai fini del presente regolamento si applicano le definizioni di cui all'articolo 4 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), di seguito denominato RGPD.

2. In aggiunta a quanto previsto al comma 1, ai fini del presente regolamento, si intende per:

a) registro tumori: un sistema attivo di raccolta sistematica di dati personali anagrafici e sanitari dei casi di tumore che insorgono nei residenti nel territorio della Regione Toscana, realizzato ai fini di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, nonché di elaborazione delle informazioni epidemiologiche e statistiche a supporto delle attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;

b) tumore (neoplasia, cancro, malattia oncologica): malattia a carattere evolutivo, come descritta dai codici 140 – 239 della Classificazione Internazionale delle malattie e cause di morte IX Revisione ovvero dai codici C00-C97 e D00-D48 della Classificazione Internazionale delle Malattie e Cause di morte, X edizione, OMS, 1992, ovvero tutte le lesioni comprese nelle diverse edizioni e revisioni della Classificazione Internazionale delle Malattie per l'Oncologia (ICD-O).

Art. 2

Oggetto del regolamento

1. Nell'ambito delle finalità di rilevante interesse pubblico previste alle lettere v) e cc) del comma 2 dell'articolo 2-sexies del decreto legislativo giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), il presente regolamento, ai sensi dell'articolo 20 ter della legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale) disciplina le specifiche finalità perseguite dal registro tumori della regione, i tipi di dati sensibili trattati e le operazioni eseguibili, i soggetti che possono trattare i dati medesimi nonché le misure per la sicurezza dei dati.

Art. 3

Finalità specifiche del trattamento di dati

1. Nell’ambito delle finalità di rilevante interesse pubblico di cui all’articolo 2, il registro tumori è finalizzato a:

a) produrre misure dell’incidenza, mortalità, sopravvivenza e prevalenza dei tumori;

b) descrivere il rischio della malattia per sede e per tipo di tumore, età, genere ed ogni altra variabile di interesse per la ricerca scientifica;

c) svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio dei tumori, sugli esiti degli interventi di diagnosi precoce, delle terapie e dei percorsi diagnostico-terapeutici, anche in collaborazione con altri enti e strutture regionali, nazionali e internazionali di ricerca scientifica in campo epidemiologico;

d) produrre dati anonimi e aggregati per la programmazione, gestione, controllo e valutazione dell’assistenza sanitaria, inerente gli interventi di prevenzione primaria e secondaria rivolti alle persone ed all’ambiente di vita e lavoro, nonché dell’efficacia dei programmi di screening;

e) monitorare e valutare i dati relativi all'appropriatezza e qualità dei servizi diagnostici terapeutici, alla sopravvivenza dei pazienti affetti da cancro.

Art. 4

Titolare del trattamento dei dati

1. Titolare del trattamento dei dati personali contenuti nel registro tumori è l’Istituto per lo studio, la prevenzione e la rete oncologica (ISPRO), ente del servizio sanitario regionale di cui alla legge regionale 14 dicembre 2017, n. 74 (Disciplina dell'Istituto per lo studio, la prevenzione e la rete oncologica), presso cui è istituito il registro.

2. Nell’ambito delle finalità di cui all’articolo 3, ISPRO garantisce la gestione amministrativa, tecnica ed informatica del registro tumori.

Art. 5
Tipi di dati sensibili trattati

1. Per il perseguimento delle finalità di cui all'articolo 3, il titolare del trattamento del registro tumori tratta dati personali idonei a rivelare lo stato di salute riferiti a casi diagnosticati di tumore, nei limiti di quanto indispensabile per il raggiungimento delle predette finalità e nei modi previsti all'articolo 10, nonché nel rispetto delle previsioni delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, di cui all'allegato A 4 del d. lgs 196/2003, in quanto compatibili.

2. Il titolare del trattamento del registro tumori tratta i seguenti dati:

a) diagnosi e modalità di ammissione e dimissione, relative a ricoveri e a prestazioni ambulatoriali diagnostico terapeutiche e rispettivi D.R.G (Diagnosis Related Groups)

b) anamnesi;

c) interventi chirurgici e procedure diagnostiche e terapeutiche, ivi compresi gli screening oncologici;

d) indagini cliniche e trattamenti eseguiti;

e) referti di anatomia patologica;

f) data e causa di morte e condizioni morbose rilevanti per il decesso.

Art. 6
Fonti dei dati

1. Il titolare del trattamento del registro tumori effettua la raccolta dei dati di cui all'articolo 5, comma 2, riferiti ai casi diagnosticati di tumore, con le modalità e nel rispetto delle misure di sicurezza dettagliate nel disciplinare tecnico di cui all'allegato A, presso:

a) l’archivio regionale/provinciale delle schede di dimissioni ospedaliere (SDO), contenenti diagnosi di tumore o relative ai soggetti iscritti o da iscrivere nel Registro Tumori, al fine di individuare nuovi casi non registrati ovvero, ove necessario, verificare i dati già inseriti nel registro medesimo;

b) i seguenti archivi delle aziende sanitarie, degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e delle strutture sanitarie private accreditate, limitatamente alle informazioni ivi contenute correlate alle patologie tumorali, al fine di implementare il registro con riferimento ai casi segnalati ed aggiornare il registro tumori con l’inserimento di eventuali ulteriori casi:

1) archivi delle schede di morte relativamente ai soggetti con diagnosi di neoplasia definita dal registro tumori e ai soggetti con neoplasia come causa di morte o condizione morbosa rilevante per il decesso;

2) archivi delle cartelle cliniche;

3) archivi di anatomia patologica;

4) archivi di laboratorio e di radiodiagnostica;

5) archivi delle prestazioni ambulatoriali;

6) archivi delle prescrizioni farmaceutiche;

7) archivi delle esenzioni ticket per patologia oncologica;

8) archivi delle protesi di interesse oncologico;

9) archivi delle prestazioni di riabilitazione di interesse oncologico;

10) archivio delle vaccinazioni di interesse oncologico;

11) lettere di dimissioni ospedaliere e relazioni cliniche.

c) l’anagrafe sanitaria regionale degli assistiti per effettuare il raffronto dei dati anagrafici dei soggetti iscritti o da iscrivere nel registro tumori con i dati anagrafici contenuti nella predetta anagrafe, al fine di verificarne ove necessario l’esattezza e l’aggiornamento dei dati e individuare eventuali duplicazioni.

2. I soggetti individuati al comma 1 devono trasmettere le informazioni di cui all’articolo 5, comma 2 secondo le modalità specificate ai sensi del disciplinare tecnico di cui all'allegato A.

Art. 7
Comunicazione dei dati

1. Il titolare del trattamento del registro tumori, per le finalità di cui all’articolo 3, può comunicare le informazioni di cui all’articolo 5, comma 2, ai titolari del trattamento dei dati dei registri tumori di altre regioni, qualora legittimamente istituiti e regolamentati ai sensi dell’articolo 2-sexies del d.lgs. 196/2003 e previa stipula di apposita convenzione che definisca le modalità tecniche di trasmissione dei dati medesimi in conformità alle misure di sicurezza individuate nell’allegato 2 del Provvedimento del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015. Tali modalità devono garantire un livello di sicurezza adeguato equivalente a quello assicurato dalle misure specificate nel disciplinare tecnico previsto dall’articolo 10.

2. Il titolare del trattamento del registro tumori, per l’esclusivo perseguimento delle finalità di cui all'articolo 3, può svolgere studi in campo medico, biomedico ed epidemiologico, anche in collaborazione con Università, Enti ed Istituti di ricerca e società scientifiche, nonché con ricercatori, singoli o associati, che operano nell’ambito delle predette Università, Enti ed Istituti di ricerca e società scientifiche, nel rispetto delle delle previsioni delle regole deontologiche per trattamenti a fini statistici o di ricerca scientifica di cui all'allegato A.4 al d.lgs. 196/2003.

Art. 8
Diffusione dei dati

1. Il titolare del trattamento del registro tumori, per le finalità di cui all’articolo 3, diffonde, anche mediante pubblicazione, dati anonimi relativi ai casi registrati in forma esclusivamente aggregata oppure secondo modalità che non rendano identificabili i soggetti interessati.

Art. 9

Operatori del registro tumori

1. I dati personali contenuti nel registro tumori sono trattati in modo lecito, corretto e trasparente, secondo i principi di cui all’articolo 5 del RGPD, soltanto da personale appositamente individuato dal titolare del trattamento, in conformità all’articolo 29 del RGPD e dell’articolo 2-quaterdecies del d.lgs. 196/2003 e sottoposto a regole di condotta analoghe al segreto professionale stabilite dal titolare del trattamento qualora non sia tenuto per legge al segreto professionale.

2. I soggetti di cui al comma 1 accedono ai dati del registro tumori secondo modalità e logiche di elaborazione strettamente pertinenti e non eccedenti ai compiti attribuiti a ciascuno di essi.

Art. 10

Misure di sicurezza

1. Il titolare del trattamento del registro tumori adotta ai sensi dell’articolo 32 del RGPD adeguate modalità tecniche e misure di sicurezza dei dati e dei sistemi, specificate nel disciplinare tecnico contenuto nell'allegato A).
2. La sicurezza dei dati trattati dal registro t deve essere garantita in tutte le fasi del trattamento dei dati, mediante l’adozione degli opportuni accorgimenti volti a preservare i medesimi dati da rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 11

Codifica dei dati trattati

1. I dati sensibili contenuti nel registro tumori, tenuti con l’ausilio di strumenti elettronici, sono trattati mediante l’utilizzo di codici identificativi, nel rispetto di quanto stabilito dal disciplinare tecnico di cui all’allegato A, in modo tale da tutelare l’identità e la riservatezza degli interessati nel trattamento dei dati, rendendoli temporaneamente inintelleggibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità.

2. I dati idonei a rivelare lo stato di salute sono trasmessi al registro e conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 1 anche quando sono tenuti senza l'ausilio di strumenti elettronici.

Art. 12
Informativa agli interessati

1. Il titolare del trattamento dei dati del registro tumori deve fornire l'informativa agli interessati per il tramite delle strutture del servizio sanitario regionale, pubbliche o private accreditate che erogano le prestazioni sanitarie, nelle modalità previste dagli articoli 13 e 14 del RGPD ed è tenuto a garantire agli interessati il pieno e tempestivo esercizio dei diritti previsti da tali articoli.

Art. 13
Notifica di violazione dei dati personali

1. Nel caso in cui i dati trattati nell'ambito del registro tumori subiscano violazioni tali da comportare la perdita, la distruzione o la diffusione indebita di dati personali, il titolare del trattamento effettua una notifica al Garante per la protezione dei dati personali nei termini e secondo le modalità previste dall'articolo 33 del RGPD. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica le violazioni all'interessato senza ingiustificato ritardo, con le modalità previste dall'articolo 34 del RGPD.

Art. 14
Norme transitorie

1. L'adeguamento e l'adozione delle modalità tecniche e delle misure di sicurezza contenute nel disciplinare tecnico di cui all'allegato A, devono avvenire entro centottanta giorni dall'entrata in vigore del presente Regolamento.

Art. 15

Entrata in vigore

1. Il presente regolamento entra in vigore il giorno successivo alla pubblicazione sul Bollettino Ufficiale della Regione Toscana.

Allegato A.

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

Premessa

In relazione alle misure di sicurezza di cui all'articolo 32 del RGPD, il presente disciplinare specifica:

A. le modalità tecniche di raccolta dei dati di cui all'art. 5 comma 2 presso gli archivi individuati all'articolo 6 del Regolamento, che può avvenire mediante:

a) invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web (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.

B. 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'art.30 del D.Lgs.vo 30 giugno 2003, n.196, 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 sensibili 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 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'art. 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 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. nella fase transitoria di cui all'articolo 14 del Regolamento, necessaria per l'adeguamento tecnologico, la password 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.5. 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’art.6, comma 2, del Regolamento, per estrapolare i dati destinati ad alimentare e ad aggiornare il Registro stesso;

c.6. sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;

c.7. sia vietato l’utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;

c.8. 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;

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

1.2 Invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web (web services) o cooperazione applicativa)

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, degli istituti di ricovero e cura a carattere scientifico e delle 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/Provincia, 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 recante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015".

1.3 Accesso diretto degli incaricati del Registro Tumori ai sistemi informatici delle strutture sanitarie di cui all’articolo 6 del Regolamento

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’art. 6 del regolamento.

1.4 Trasmissione su supporti informatici (es. CD, DVD, memorie a stato solido)

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’ Ufficio “XXX””;

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.

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

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. Nella fase transitoria di cui all’articolo 14 del Regolamento necessaria per l’adeguamento tecnologico a tale soluzione, non superiore a 180 giorni dall’entrata in vigore del Regolamento, è possibile utilizzare credenziali costituite da codice identificativo e parola chiave riservata robusta, univoca, non condivisa, modificata con cadenza massima di 90 giorni;

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 ed 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 ed uscita di tali persone.

5. MANUTENZIONDE DEI SISTEMI INFORMATICI

5.1. Nel rispetto di quanto prescritto dall'art.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, in conformità a quanto stabilito dal punto 25 dell'Allegato B del Decreto Legislativo 30 giugno 2003, n. 196, 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 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 etc..) 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.