

Regolamento recante norme per il funzionamento del Registro Tumori della Regione Friuli Venezia Giulia.

- Art. 1 Definizioni
- Art. 2 Oggetto del regolamento
- Art. 3 Finalità specifiche del trattamento di dati
- Art. 4 Titolare e responsabile del trattamento dei dati
- Art. 5 Tipi di dati sensibili trattati
- Art. 6 Fonti dei dati
- Art. 7 Comunicazione dei dati
- Art. 8 Diffusione dei dati
- Art. 9 Operatori del Registro Tumori Regionale
- Art. 10 Misure di sicurezza
- Art. 11 Codifica dei dati
- Art. 12 Informativa agli interessati
- Art. 13 Data breach
- Art. 14 Norme transitorie
- Art. 15 Conservazione dei dati trattati
- Art. 16 Entrata in vigore

Allegato A

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

Art. 1 Definizioni

1. Ai fini del presente Regolamento si applicano le definizioni di cui all'articolo 4 del Regolamento del Parlamento europeo e del Consiglio 2016/679 del 27 aprile 2016 (General Data Protection Regulation), di seguito GDPR, e dell'articolo 1, comma 1, del decreto del Ministro della Salute 1 agosto 2023 (Registro nazionale tumori).

2. In aggiunta a quanto previsto al comma 1, si intende per <<Registro Tumori Regionale>> un sistema attivo di raccolta sistematica di dati personali anagrafici e sanitari dei casi di tumore che insorgono nei residenti nel territorio della Regione Friuli Venezia Giulia, 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.

Art. 2 oggetto del regolamento

1. Nell'ambito delle finalità di rilevante interesse pubblico previste dall'articolo 2-sexies, comma 2, lettere t), u), v) e cc) 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) 2016/679, 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), il presente regolamento, ai sensi dell'articolo 35 della legge regionale 26 ottobre 2006, n. 19 (Disposizioni in materia di salute umana e sanità veterinaria e altre disposizioni per il settore sanitario e sociale, nonché in materia di personale) disciplina le specifiche finalità perseguite dal Registro Tumori della Regione, i tipi di dati 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. Fatto salvo quanto previsto dalla vigente normativa di settore e, in particolare, dal decreto del Presidente del Consiglio dei Ministri 3 marzo 2017 (Identificazione dei sistemi di sorveglianza e dei registri di mortalità, di tumori e di altre patologie) e dal citato decreto del Ministro della Salute 1 agosto 2023, il Registro Tumori Regionale, nell'ambito delle finalità di rilevante interesse pubblico di cui all'articolo 2 del presente regolamento, 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 tumore.

Art. 4 Titolare e responsabile del trattamento dei dati

1. Titolare del trattamento dei dati personali contenuti nel Registro Tumori Regionale è l'Istituto di Ricovero e Cura a Carattere Scientifico "Centro di riferimento oncologico" di Aviano (PN) presso cui è istituito il Centro di riferimento del Registro Tumori Friuli Venezia Giulia, il quale assicura la tenuta del registro e ogni altra relativa attività di natura tecnica e amministrativa.

2. I dati del Registro Tumori regionale sono messi a disposizione della Regione Friuli Venezia Giulia dal Centro di riferimento regionale per finalità di governo e programmazione sanitaria, nei limiti delle competenze attribuite dalla legge ed esclusivamente mediante un sistema di codifica che non consente l'identificazione diretta dell'interessato, secondo quanto previsto dall'articolo 5, comma 4, del decreto del Presidente del Consiglio dei ministri 3 marzo 2017.

3. La società INSIEL Spa, incaricata della gestione dell'infrastruttura informatica del Registro tumori regionale, è nominata responsabile del trattamento ai sensi dell'articolo 28 del GDPR.

Art. 5 Tipi di dati sensibili trattati

1. Per il perseguimento delle finalità di cui all'articolo 3 del presente regolamento, il Titolare del trattamento del Registro Tumori Regionale tratta dati 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 del presente regolamento, nonché nel rispetto delle previsioni del Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, ai sensi dell'articolo 106 del decreto legislativo 196/2003, in quanto compatibili.

2. Il Titolare del trattamento del Registro Tumori Regionale 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 Regionale effettua, per il tramite del Responsabile del Trattamento, la raccolta dei dati di cui all'articolo 5, comma 2, del presente regolamento, riferiti ai casi diagnosticati di tumore, con le modalità e nel rispetto delle misure di sicurezza di cui all'articolo 32 del GDPR, come dettagliate nel Disciplinare tecnico di cui all'articolo 10, presso:

a) L'archivio regionale delle Schede di dimissioni ospedaliere (SDO), contenenti diagnosi di tumore o relative ai soggetti iscritti o da iscrivere nel Registro Tumori Regionale, 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 regionali, degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e delle strutture sanitarie private accreditate della Regione, 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 Regionale con l'inserimento di eventuali ulteriori casi:

- 1) archivi delle schede di morte relativamente ai soggetti con diagnosi di neoplasia definita dal Registro tumori Regionale e ai soggetti con neoplasia come causa di morte o condizione morbosa rilevante per il decesso;
- 2) archivi delle cartelle cliniche, compresa la cartella oncologica;
- 3) archivi di Anatomia Patologica;
- 4) archivi di laboratorio;
- 5) archivi delle prestazioni ambulatoriali;
- 6) archivi delle prescrizioni farmaceutiche;
- 7) archivi delle esenzioni ticket per patologia oncologica;
- 8) archivi delle prestazioni di riabilitazione di interesse oncologico;
- 9) 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 Regionale 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 del presente regolamento, secondo le modalità specificate ai sensi del Disciplinare tecnico previsto dall'articolo 10 del presente regolamento.

Art. 7 Comunicazione dei dati

1. Il Titolare del trattamento del Registro Tumori Regionale, per le finalità di cui all'articolo 3 del presente regolamento, 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'art. 2-ter, commi 3 e 4 del decreto legislativo 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, pubblicato sulla G.U. n. 179 del 4 agosto 2015. Tali modalità devono garantire un livello di sicurezza equivalente a quello assicurato dalle misure specificate nel Disciplinare Tecnico previsto dall'articolo 10 del presente regolamento.
2. Il Titolare del trattamento del Registro Tumori Regionale, per l'esclusivo perseguimento delle finalità di cui all'articolo 3 del presente Regolamento, 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 regole previste dal Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici di cui all'allegato A.4 al decreto legislativo 196/2003.
3. Il Titolare del trattamento del Registro Tumori Regionale attua quanto previsto dagli articoli 9 e 10 del decreto del Ministro della Salute 1 agosto 2023.

Art. 8 Diffusione dei dati

1. Il Titolare del trattamento del Registro Tumori Regionale, per le finalità di cui all'articolo 3 del presente regolamento, diffonde, anche mediante la pubblicazione sul proprio sito internet istituzionale, dati anonimi ovvero anonimizzati relativi ai casi raccolti e registrati in forma esclusivamente aggregata ed in ogni caso secondo modalità che non rendano in modo alcuno identificabili i soggetti interessati.

Art. 9 Operatori del Registro Tumori Regionale

1. I dati personali contenuti nel Registro Tumori Regionale sono trattati, nel rispetto dei principi di indispensabilità, necessità, pertinenza e non eccedenza di cui al GDPR e al decreto legislativo 196/2003, soltanto da personale appositamente individuato e autorizzato dal Titolare del trattamento e dal Responsabile del Trattamento, in conformità all'articolo 29 del GDPR e all'art. 2-quaterdecies del decreto legislativo 196/2003.
2. I soggetti autorizzati al trattamento dei dati sono sottoposti a regole di condotta analoghe al segreto professionale stabilite dal Titolare del trattamento qualora non siano tenuti per legge al segreto professionale, ed accedono ai dati del Registro Tumori Regionale 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 Regionale adotta le modalità tecniche e le misure di sicurezza dei dati e dei sistemi di cui all'articolo 32 del GDPR, meglio specificate nel Disciplinare Tecnico contenuto nell'Allegato A) al presente regolamento, che costituisce sua parte integrante e sostanziale.
2. La sicurezza dei dati trattati dal Registro Tumori Regionale 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 particolari contenuti nel Registro Tumori Regionale sono trattati, con l'ausilio di strumenti elettronici, mediante l'utilizzo di codici identificativi, nel rispetto di quanto stabilito dal Disciplinare tecnico contenuto nell'Allegato A al presente regolamento, in modo tale da tutelare l'identità e la riservatezza degli interessati nel trattamento dei dati, nel rispetto della normativa vigente.

2. I dati idonei a rivelare lo stato di salute sono trasmessi al Registro Tumori Regionale 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 precedente comma 1 anche quando sono tenuti senza l'ausilio di strumenti elettronici, così come previsto dalla normativa vigente.

Art. 12 Informativa agli interessati

1. Il Titolare del trattamento dei dati del Registro Tumori Regionale 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 artt. 13 e 14 del GDPR ed è tenuto a garantire agli interessati il pieno e tempestivo esercizio dei diritti previsti dal medesimo GDPR.

Art. 13 Data breach

1. Sono notificate al Garante per la protezione dei dati personali, senza ingiustificato ritardo e comunque entro settantadue ore dall'avvenuta conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali oggetto di trattamento per la tenuta e il funzionamento del Registro Tumori Regionale (c.d. *data breach*) con le modalità previste dall'articolo 33 del GDPR.

2. 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 GDPR.

Art. 14 Norme transitorie

1. L'adeguamento e l'adozione delle modalità tecniche e delle misure di sicurezza di cui al Disciplinare Tecnico previsto dall'articolo 10, devono avvenire entro 180 giorni dall'entrata in vigore del presente regolamento.

Art. 15 Conservazione dei dati trattati

1. I dati personali presenti nel Registro Regionale Tumori sono cancellati trascorsi centoventi anni dal decesso dell'interessato.

Art. 16 Entrata in vigore

1. Il presente regolamento entra in vigore il giorno successivo alla sua pubblicazione sul Bollettino ufficiale della Regione Friuli Venezia Giulia.

Allegato A

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

Premessa

Il Registro Tumori Regionale è realizzato su un'infrastruttura collocata all'interno del data center regionale gestito dalla società in house INSIEL Spa. ed è alimentato dalle fonti dati di cui all'art. 6 del Regolamento e presenti nel sistema informatico socio sanitario regionale - SSSR.

L'accesso al registro da parte del Titolare e suoi soggetti autorizzati al trattamento avviene tramite applicazione WEB.

Ferme restando le misure di sicurezza, individuate negli articoli 32 e 36 del GDPR, il presente Disciplinare specifica:

a) le modalità tecniche di trasmissione dei dati al Registro Tumori Regionale da parte dei soggetti individuati all'articolo 6 del Regolamento, che può avvenire mediante:

- 1) invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web (web services) o cooperazione applicativa;
- 2) accesso diretto dei soggetti autorizzati al trattamento del Registro Tumori Regionale ai sistemi informatici delle strutture sanitarie di cui all'articolo 6 del Regolamento;
- 3) trasmissione su supporti informatici (ad es. CD, DVD, memorie a stato solido);
- 4) trasmissione di documenti cartacei in plico chiuso e sigillato nelle more della messa a regime delle modalità di cui ai numeri 1), 2) e 3).

I supporti di cui ai numeri 3) e 4) sono utilizzati esclusivamente per estrapolare i dati da inserire nel Registro Tumori Regionale

b) le misure di sicurezza che:

- 1) il Titolare del trattamento dei dati del Registro Tumori Regionale e il Responsabile del trattamento, nominato ai sensi dell'articolo 28 del GDPR, devono adottare per il funzionamento del registro medesimo;
- 2) le strutture presso le quali sono raccolti i dati che alimentano il Registro Tumori Regionale, quali la Regione (per l'anagrafe sanitaria regionale), 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.

DESCRIZIONE DEL SISTEMA INFORMATICO

Per garantire la protezione del patrimonio informativo del Registro Tumori Regionale sono attivate misure di sicurezza fisica e logica idonee a salvaguardare l'integrità e la riservatezza delle informazioni.

Misure idonee a garantire la protezione dei dati, quali:

- isolamento logico della rete;
- protezione dei dati e delle applicazioni da danneggiamenti provocati da virus informatici;
- autenticazione degli utenti;
- controllo dell'accesso alle applicazioni ed ai dati;

La sicurezza è incrementata mediante l'adozione di:

- servizi di firewall e proxy;
- strumenti IPS/IDS (Intrusion Prevention System/Intrusion Detection System);
- sistema di gestione degli accessi e di profilazione utenti;
- sistema di registrazione delle operazioni di accesso degli utenti ai sistemi e delle operazioni di trattamento, al fine di permettere l'individuazione di eventuali anomalie;
- un servizio di Log Management che realizza le attività di logging, monitoraggio e correlazione degli eventi di sicurezza;
- un servizio di gestione Antivirus e Host IPS che centralizza la gestione delle componenti antivirus e HIPS (Host Intrusion Prevention System);

- uno strumento di controllo per l'accesso degli amministratori di sistema e per la gestione dei privilegi di accesso da parte degli amministratori delle basi di dati;

Misure idonee a garantire la continuità del servizio, quali:

Il datacenter di Insiel è certificato TIA-942 Rated-3 in relazione agli standard di affidabilità dell'infrastruttura e a garanzia nella continuità dei servizi. In particolare, sono previsti sistemi in alta affidabilità quali:

- impianti elettrici, di condizionamento e di rete;
- UPS e gruppi di continuità;

Per garantire la disponibilità del Registro Tumori Regionale nel tempo sono attive diverse procedure quali:

- salvataggio periodico dei dati (backup sia incrementale che storico);
- data recovery;

L'accesso fisico al datacenter è controllato e gestito in modalità H24 da personale. L'accesso ai sistemi è consentito solo mediante autorizzazione.

DISPOSIZIONI GENERALI

Il Titolare del trattamento dei dati del Registro Tumori Regionale e il Responsabile del trattamento, nominato ai sensi dell'articolo 28 del GDPR, istruiscono i rispettivi soggetti autorizzati al trattamento dei dati, individuati ai sensi della normativa vigente in materia di protezione dei dati personali, 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 Regionale 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 Regionale, sono dotate di:

- a) sistemi antivirus 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 Regionale, per il tramite del Responsabile del trattamento, 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 Regionale. Verifica inoltre l'esattezza e l'aggiornamento dei dati anagrafici dei soggetti iscritti o da iscrivere nel Registro Tumori Regionale mediante il raffronto con i dati contenuti nel data base dell'Anagrafe 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 autorizzato al 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 autorizzato al trattamento dei dati nonché per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati garantendo che:

- 1) la raccolta dei dati avvenga soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP del Titolare del trattamento del Registro Tumori Regionale o dotate di certificato digitale, emesso da una Certification Authority ufficiale, che identifichi univocamente la postazione di lavoro;
 - 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;
 - 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;
 - 4) nella fase transitoria di cui all'articolo 14 del Regolamento, necessaria per l'adeguamento tecnologico, la password venga consegnata al singolo soggetto autorizzato al trattamento, separatamente rispetto al codice per l'identificazione e sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi;
 - 5) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;
 - 6) sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;
 - 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 dei soggetti autorizzati al trattamento. 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 formato e autorizzato al 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 di 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 Regionale 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 Regionale; 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 strumenti di cui al punto b).

Il Titolare del trattamento dei dati del Registro Tumori Regionale è tenuto a stipulare una convenzione (o altro atto bilaterale) con ciascuno dei soggetti di cui all'articolo 6 del regolamento, secondo uno schema tipo predisposto dalla Regione, 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 dei soggetti autorizzati del Registro Tumori Regionale ai sistemi informatici delle strutture sanitarie di cui all'articolo 6 del Regolamento.

L'accesso non è diretto ma la raccolta delle informazioni avviene per il tramite del Responsabile del trattamento.

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

Il Titolare del trattamento dei dati del Registro Tumori Regionale, 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 Regionale, 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 autorizzati al 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.

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

2. FASE DI ELABORAZIONE DEI DATI

2.1 Ai fini dell'attuazione di quanto previsto all'articolo 11 del Regolamento, il sistema di codifica di tutti i dati memorizzati su file/database presso il Registro Tumori Regionale prevede l'utilizzo di tecniche di pseudoanonimizzazione.

2.2 I dati raccolti nel Registro Tumori Regionale sono trattati dai soggetti autorizzati al trattamento del Registro Tumori Regionale esclusivamente attraverso applicazioni software dotate di adeguati sistemi di autenticazione e di autorizzazione in funzione del ruolo dei soggetti autorizzati al trattamento 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. 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 Regionale 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 Regionale, codificati ai sensi dei punti 2.1, 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.

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 dai soggetti autorizzati al trattamento 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 REGIONALE

4.1. L'accesso ai locali del Registro Tumori Regionale, 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. MANUTENZIONE DEI SISTEMI INFORMATICI

5.1. Nel rispetto di quanto prescritto dall'articolo 28 del GDPR, i soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici, che possono comportare il trattamento dei dati del Registro Tumori Regionale, 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 dall'articolo 28 del GDPR, 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 Regionale devono essere cancellati o resi anonimi in maniera irreversibile nel sistema informatico medesimo, trascorso un periodo di 120 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 Regionale 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 (e misure di sicurezza dei dati personali (G.U. n. 287 del 9 dicembre 2008).

6.4. I supporti cartacei del Registro Tumori Regionale, 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.

IL SEGRETARIO GENERALE

IL PRESIDENTE