CONFERENZA DELLE REGIONI
E DELLE PROVINCE AUTONOME

22/65/CR10/C1-C7

PROGETTO DI REGOLAMENTO REGISTRO MALATTIE RARE E RELATIVO DISCIPLINARE TECNICO

Roma, 13 aprile 2022

Schema tipo di Regolamento Registro Malattie Rare.

Sommario

Art. 1 – Definizioni

1. Ai fini del presente Regolamento si applicano le definizioni di cui all'articolo 4 del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679.

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

a) Malattia Rara: una patologia che colpisce meno di una persona su 2000 nel territorio della Comunità Europea. L'elenco di riferimento delle malattie rare a livello europeo è definito e mantenuto da Orphanet;

b) Registro Malattie Rare: un sistema attivo di raccolta sistematica di dati personali anagrafici e sanitari dei casi di malattie rare che insorgono nei residenti nel territorio di (……),

nonché quelle che colpiscono pazienti provenienti da altre Regioni, Province Autonome o da altri Stati e che sono diagnosticati e/o presi in carico presso i Centri della Rete per le Malattie Rare della Regione/PA.

Art. 2 – Oggetto del regolamento

1. Il presente regolamento disciplina il Registro Malattie Rare della Regione, di cui al DPCM 03.03.2017 e alla ……(atto regionale), identificando i tipi di dati e le operazioni eseguibili da parte della Giunta regionale, nonché da parte delle aziende sanitarie della Regione/Provincia.

CAPO I -Trattamenti per finalità di cura

Art. 3 – Titolari del trattamento

1. Per le finalità di cura sono Titolari del trattamento i soggetti e gli esercenti le professioni sanitarie che prendono in cura **l'assistito** sia nell'ambito del SSN e dei servizi socio-sanitari regionali, sia al di fuori degli stessi.

Art. 4 – Tipologia di Dati trattati

1. I dati trattati dai soggetti di cui all'art. 3 del presente regolamento sono costituiti dall'anagrafica dell'assistito e da dati di natura particolare ex art. 9 del Regolamento UE 2016/679, ovvero dati relativi allo stato di salute degli assistiti e specificatamente:

a) sospetto diagnostico, screening, diagnosi, dati clinici, strumentali, di laboratorio, inclusi i test genetici, finalizzati alla diagnosi, al trattamento, al monitoraggio e alla prevenzione di ulteriori aggravamenti;

b) terapie di qualsiasi natura, farmacologica e non, relativi alla persona con malattia rara;

c) diagnosi e modalità di ammissione e dimissione, relative a ricoveri e a prestazioni ambulatoriali diagnostico terapeutiche;

d) anamnesi, compresa quella familiare;

e) indagini cliniche —ad includere dati di laboratorio, strumentali, referti di anatomia patologica, test genetici— e trattamenti eseguiti;

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

Art. 5 – Liceità del trattamento

1. I soggetti del Servizio sanitario nazionale e dei servizi sociosanitari regionali, nonché gli esercenti le professioni sanitarie, ancorché soggetti al segreto professionale o comunque all'obbligo di segretezza, effettuano trattamenti dei dati personali di cui all'articolo precedente per "finalità di cura" in aderenza all'art. 9, par. 2, lett. h) e par. 3 del Regolamento UE 2016/679.

CAPO II -Trattamenti per finalità di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico

Art. 6 – Titolare del trattamento

La Regione/Provincia, Aziende unità sanitarie locali, Aziende ospedaliere, Istituti di ricerca e cura a carattere scientifico, Aziende universitarie di qualsiasi tipo e natura operanti nell'ambito del Servizio sanitario nazionale, effettuano trattamenti di dati personali per le seguenti finalità:

a) produrre stime epidemiologiche di occorrenza e di rischio grezzo e specifico per singole malattie rare, per gruppi omogenei di patologie e per le malattie rare nel loro complesso;
b) svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio connessi a specifiche malattie rare
c) produrre studi scientifici, anche in collaborazione con altri enti e strutture regionali, nazionali e internazionali.

Art. 7 – Tipologia di dati trattati

1. I Titolari del trattamento di cui all'articolo precedente trattano i dati degli assistiti indicati all'art. 4 del presente Regolamento privati dei dati identificativi diretti dell'assistito e nel rispetto principi di minimizzazione dei dati, necessità, pertinenza e non eccedenza. in relazione alle finalità di cui all'articolo che precede.

Art. 8 – Liceità del trattamento

1. La Regione/Provincia e le Aziende unità sanitarie locali, Aziende ospedaliere, Istituti di ricerca e cura a carattere scientifico, Aziende universitarie di qualsiasi tipo e natura operanti nell'ambito del Servizio sanitario nazionale svolgono attività di ricerca scientifica e di studi epidemiologici, poiché ritenute finalità di rilevante interesse pubblico, utilizzando i dati personali presenti nel Registro delle Malattie Rare ed analizzando, a titolo esemplificativo e non esaustivo, gli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio delle patologie di rilevante interesse regionale, gli 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.

CAPO III -Trattamenti per finalità di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria

Art. 9 – Titolare del trattamento

1. Per le finalità di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria titolare del trattamento sono:

a) la Regione/Provincia,
b) Aziende unità sanitarie locali, Aziende ospedaliere, Istituti di ricerca e cura a carattere scientifico, Aziende universitarie di qualsiasi tipo e natura operanti nell'ambito del Servizio sanitario nazionale.

2. I soggetti di cui alla lettera b) perseguono le finalità di cui al comma 1 limitatamente ai servizi sanitari erogati.

Art. 10 – Tipologia di dati trattati

1. I Titolari del trattamento di cui all'articolo precedente trattano i dati degli assistiti indicati all'art. 4 del presente Regolamento privati dei dati identificativi diretti dell'assistito e nel rispetto principi di minimizzazione dei dati, necessità, pertinenza e non eccedenza. in relazione alle finalità di cui all'articolo che precede.

Art. 11 – Liceità del trattamento

La Regione_____ e le Aziende ospedaliere, Istituti di ricerca e cura a carattere scientifico, Aziende universitarie di qualsiasi tipo e natura operanti nell'ambito del Servizio sanitario nazionale svolgono attività di programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria, poiché ritenute finalità di rilevante interesse pubblico, utilizzando i dati personali presenti nei registri di patologie di rilevante interesse regionale valutando gli impatti di salute conseguenti ad attività di pianificazione sul territorio, ovvero di bonifica o interventi di adattamento (ad es. per far fronte agli effetti sulla salute dei cambiamenti climatici). I soggetti di cui alla lettera b) del comma 2 dell'art. 9 del presente

regolamento perseguono le finalità di cui al comma 1 limitatamente al perimetro di propria competenza.

CAPO IV -Fonti di dati e flussi comunicativi

Art. 12 – Fonti dei dati

1. Nel Registro Malattie Rare confluiscono i dati dalle fonti di seguito indicate:

a) censimento attivo dei casi di malattia rara da parte degli operatori dei Centri di riferimento individuati dalle Regioni/Province Autonome nell'ambito della rete malattie rare e/o da parte degli operatori incaricati delle ASL di residenza nel caso di pazienti seguiti per la diagnosi e/o piano terapeutico da Centri di riferimento della rete malattie rare di altra Regione o Provincia autonoma;

b) dati dell'archivio dell'anagrafe sanitaria regionale/provinciale, delle Aziende sanitarie, degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e delle strutture sanitarie private accreditate, già in forma pseudonimizzata, anche al fine di individuare nuovi casi non registrati ovvero, ove necessario verificare i dati già inseriti nel Registro medesimo e di permettere la raccolta delle informazioni sulle terapie in atto e sull'evoluzione della malattia;

c) dati dell'archivio regionale/provinciale delle Schede di dimissioni ospedaliere (SDO);

d) dati dell'archivio regionale/provinciale dei soggetti aventi un'esenzione dalla spesa sanitaria per malattia rara inclusa nell'elenco del Decreto del Ministero della salute 18 maggio 2001, n 279 e nei successivi aggiornamenti nazionali ed integrazioni Regionali/Provinciali;

e) dati degli archivi delle schede di morte;

f) dati degli archivi delle cartelle cliniche, con riferimento ai soli soggetti già censiti nel Registro Malattie Rare, e a mezzo dell'identificativo pseudinomizzato;

g) dati degli archivi di Anatomia Patologica;

h) dati degli archivi dei test genetici;

i) dati dei registri delle malformazioni congenite;

l) dati degli archivi dei test di screening neonatale;

m) dati degli archivi di laboratorio e di radiodiagnostica;

n) dati degli archivi delle prestazioni ambulatoriali;

o) dati degli archivi regionali/provinciali e aziendali delle prescrizioni farmaceutiche;

p) dati degli archivi delle protesi ed ausili;

q) dati degli archivi delle prestazioni di riabilitazione;

r) dati degli archivio delle vaccinazioni;

s) dati delle lettere di dimissioni ospedaliere e relazioni cliniche.

2. Con riferimento alle fonti dalla lett. c) alla lettera s) di cui al comma precedente, tutte comprese, sono acquisiti i soli dati relativi ai soggetti già censiti nel Registro Malattie Rare.
3. Per i trattamenti di cui ai Capi I e II del presente Regolamento, la Regione/Provincia può utilizzare i dati relativi ai flussi di cui alla Scheda n. 12 del Regolamento regionale per il trattamento dei dati sensibili e giudiziari nelle modalità e con le cautele ivi previste.

Art. 13 – Comunicazione dei dati

1. La Regione/PP.AA., anche attraverso i Coordinamenti regionali/provinciali per le malattie rare o altri soggetti/enti titolari del trattamento dei dati, comunica al Ministero della Salute, all'Istituto Superiore di Sanità (Registro Nazionale Malattie Rare), ad altre agenzie ed enti nazionali ed internazionali i dati di cui agli articoli 7 del Capo II e 10 del Capo III, in conformità alla normativa vigente. In particolare, i dati saranno comunicati al Ministero della Salute in ottemperanza agli adempimenti LEA (Obbligo informativo AAU) e all'Istituto Superiore di Sanità (Registro Nazionale Malattie Rare) in attuazione dell'articolo 3, comma 3 del Decreto del Ministro della Salute del 18 maggio 2001, n. 279, dell'Accordo stato-regioni del 10 maggio 2007 e del DPCM 03.03.2017.

2. La Regione/PP.AA., anche attraverso i Coordinamenti regionali/provinciali per le malattie rare o altri soggetti/enti titolari del trattamento dei dati, per le sole finalità assistenziali di cui al Capo I, ovvero nei casi di mobilità sanitaria, può comunicare i dati di cui all'art. 4 del presente Regolamento ad altra Regione o Provincia Autonoma (o altro Ente) nella qualità di Titolari del trattamento relativo al Registri Malattie Rare regionale.

3. La Regione/PP.AA., anche attraverso i Coordinamenti regionali/provinciali per le malattie rare, altri soggetti/enti titolari del trattamento dei dati e le strutture delle reti regionali per le malattie rare, per le sole finalità assistenziali di cui al Capo I, possono comunicare i dati di cui all'art. 4 del presente Regolamento agli organismi attivi a livello europeo per fornire l'assistenza programmata o urgente al malato raro che ne abbisogna e che abbia espresso il consenso, in base alla Direttiva europea 2011/24/UE.

Art. 14 – Diffusione dei dati

1. La Regione/Provincia può pubblicare e diffondere dati anonimi relativi ai casi registrati in forma esclusivamente aggregata oppure secondo modalità che non rendano in alcun modo identificabili i soggetti interessati.

CAPO V – Gestione dei registri e misure di sicurezza

Art. 15 – Gestione dei registri

1. La Regione/Provincia può assegnare la gestione del Registro ad un'Azienda unità sanitarie locali, o Azienda ospedaliere, o Istituti di ricerca e cura a carattere scientifico, o Azienda universitaria di qualsiasi tipo e natura operanti nell'ambito del Servizio sanitario nazionale.

Art. 16 – Misure di sicurezza

1. Il Registro Malattie Rare è gestito e manutenuto in aderenza al "Disciplinare tecnico in materia di misure di sicurezza per il funzionamento Registro Malattie Rare" (Appendice A del presente regolamento), il cui aggiornamento almeno biennale è demandato al Dirigente della struttura competente in materia di ICT in sanità.

Allegato A. DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FUNZIONAMENTO DEL REGISTRO MALATTIE RARE.

Premessa

Il presente Disciplinare specifica:

A) le modalità tecniche di raccolta dei dati per le finalità di cui ai capi I-II e III del Regolamento e le tipologie di dati di cui all'art.4 raccolti direttamente dai servizi di cui all'art. 12 comma 1 lettera a o presso gli archivi individuati all'articolo 12 comma 1 lettere da b a s 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) inserimento diretto da parte dei professionisti del SSR/PA coinvolti nell'assistenza al malato raro in applicativi e/o modulistica specificatamente predisposti per le finalità di cui all'art.6

c) accesso diretto degli incaricati del Registro Malattie Rare ai sistemi informatici delle strutture sanitarie di cui all'articolo 12 del Regolamento;

d) trasmissione su supporti informatici (es. CD, DVD, memorie a stato solido);

e) trasmissione di documenti cartacei in plico chiuso e sigillato nelle more della messa a regime delle modalità di cui alle lettere a), b), c) e d).

I supporti di cui alla lettera d) e e) sono utilizzati esclusivamente per estrapolare i dati da inserire nel Registro Malattie Rare.

B) le misure di sicurezza che:

a) il Titolare del trattamento del Registro Malattie Rare 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 Malattie Rare, 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 facenti parte delle reti regionali/provinciali/interregionali delle malattie rare;

devono adottare per comunicare o mettere a disposizione i dati al Titolare del trattamento.

DISPOSIZIONI GENERALI

Il Titolare del trattamento del Registro Malattie Rare istruisce gli incaricati 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 Malattie Rare 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 relativi alla salute 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 Malattie Rare, 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 **Metodologia di raccolta dei dati**

La raccolta dei dati nel registro malattie rare avviene mediante l'immissione degli stessi da parte dei professionisti/ operatori di cui all'art.12 comma a del Regolamento o mediante l'acquisizione dalle fonti indicate dall'articolo 12 del presente disciplinare.

1.2 Inserimento (o immissione?) diretto/a

I professionisti e gli operatori dei servizi di cui all'art.12 comma 1 lettera a possono raccogliere direttamente i dati e inserirli nel registro malattie rare secondo le modalità previste da ogni regione/PPAA.

Ciascun operatore e professionista in base alla ASR, servizio e ruolo svolto sarà autorizzato a raccogliere alcune tipologie di dati e a inserirli, una volta verificata la sua identità, nel registro malattie rare con modalità di volta in volta definite dalla regione/PPAA.

1.3 **Verifica dei dati raccolti e della loro sicurezza e completezza**

Il Titolare del trattamento del Registro Malattie Rare verifica con periodicità l'esattezza e l'aggiornamento dei dati anagrafici dei soggetti iscritti o da iscrivere nel Registro Malattie Rare mediante il raffronto, anche attraverso servizi di interoperabilità, con i dati contenuti nell'Anagrafe Sanitaria Regionale degli Assistibili.

1.4 Acquisizione dei dati da altre fonti

Il registro malattie rare può essere alimentato anche attraverso l'utilizzo delle fonti di cui all'art.12 comma 1 lettere da b ad s.

La raccolta dei dati presso le banche dati e gli archivi di cui all'art. 12 del Regolamento deve in ogni caso conformarsi alle seguenti modalità:

a) garantire l'accesso selettivo ai soli dati di cui all'articolo 4 del Regolamento;

b) assegnare al personale incaricato del trattamento credenziali di autenticazione e profili di autorizzazione specifici alle attività di censimento, 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 avvenga soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP della rete Malattie Rare 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, quando richiesto, 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 tracciabili 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. 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.12 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;

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

1.5 **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 Malattie Rare da parte delle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate facenti parte delle reti per le malattie rare 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 Malattie Rare; 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 relativi alla salute che devono essere riportati in appositi allegati utilizzando gli strumenti di cui al punto b).

Il Titolare del trattamento dei dati del Registro Malattie Rare è tenuto 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".**

1.6 **Accesso diretto degli incaricati del Registro Malattie Rare ai sistemi informatici delle strutture sanitarie di cui all'articolo 12 comma 1 del Regolamento**

Il Titolare del trattamento dei dati del Registro Malattie Rare, per la raccolta delle informazioni di cui all'articolo 4 effettuata con modalità informatiche direttamente dai propri incaricati presso i sistemi informatici della Regione/Provincia Autonoma, 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 Malattie Rare, abilitati ad accedere alle fonti di dati di cui all'art. 12 del regolamento.

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

Il Titolare del trattamento dei dati del Registro Malattie Rare, per la raccolta delle informazioni di cui all'articolo 4 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;

1.8 **Trasmissione di documenti cartacei**

Il Titolare del trattamento dei dati del Registro Malattie Rare, per la raccolta delle informazioni di cui all'articolo 4 effettuata mediante trasmissione di documenti cartacei, nelle ipotesi di cui alla lettera e) delle premesse, 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.

2. FASE DI ELABORAZIONE DEI DATI

2.1. Ai fini dell'attuazione di quanto previsto dal capo I (finalità di cura) del Regolamento, il dato individuale nominativo deve essere mantenuto con criptazione simmetrica basata su algoritmi biunivoci e reversibili al fine di permettere di ricostituire il dato nominativo in caso di necessità per ragioni strettamente di cura ed assistenza.

Nel caso delle finalità di cui ai capi II e III (studio e ricerca scientifica e programmazione sanitaria rispettivamente) del Regolamento il sistema di codifica dei dati identificativi degli interessati raccolti dal Registro Malattie Rare deve consistere in un numero predefinito di caratteri alfanumerici ottenuti attraverso procedure di cifratura non invertibili.

I tipi di algoritmi di cifratura da utilizzare devono essere coerenti con quanto previsto dal decreto interconnessione n.262/2016 e devono essere condivisi fra le Regioni/Provincie Autonome e Ministero della Salute, l'Istituto Superiore di Sanità, altre agenzie o Enti al fine di definire il flusso dei dati e di permettere la tracciatura pseudonimizzata dei pazienti censiti nei registri di diverse Regioni/Province autonome ed anche al fine di evitare la duplicazione dei casi nel Registro Nazionale Malattie Rare

2.2. I dati raccolti nel Registro Malattie Rare sono trattati dagli incaricati del Registro Malattie Rare 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 che includa anche una 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) 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 Malattie Rare 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 1.4 del presente disciplinare.

3. FASE DI CONSERVAZIONE DEI DATI

3.1 I dati raccolti dal Titolare del trattamento del Registro Malattie Rare, 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, 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 MALATTIE RARE

4.1. L'accesso ai locali del Registro Malattie Rare, 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'art. 28 del Regolamento UE 2016/679, i soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici, che possono comportare il trattamento dei dati del Registro Malattie Rare, 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 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 Malattie Rare devono essere cancellati o resi anonimi in maniera irreversibile trascorso un periodo di 30 anni dal decesso dell'interessato cui i dati si riferiscono, quando notificato e salvo quanto previsto dal successivo comma 4 del presente articolo.

6.2 La procedura di anonimizzazione di cui al punto precedente e relative alle finalità di cui al capo II e III del Regolamento 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.

6.3. I supporti informatici (es. memorie di massa dei server e delle postazioni di lavoro, supporti rimovibili etc..) del Registro Malattie Rare 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 Malattie Rare, 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.