Disposizioni anticipate di trattamento (DAT) di cui all'articolo 4 della l. 219/2017 (Norme in materia di consenso informato e di disposizioni anticipate di trattamento). Regolamento di attuazione dell'articolo 1, comma 1 della l.r. 13/2006 in materia di trattamento di dati sensibili e giudiziari.

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 giungo 2003, n. 196 (Codice in materia di protezione dei dati personali);

Vista la legge 22 dicembre 2017, n. 219 (Norme in materia di consenso informato e di disposizioni anticipate di trattamento) e, in particolare, l'articolo 4;

Vista la legge 27 dicembre 2017, n. 205 (Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020);

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 6 settembre 2018;

Visto il parere della competente struttura di cui all'articolo 17 del regolamento interno della Giunta regionale del 19 luglio 2016, n. 5;

Considerato quanto segue:

1. Il presente regolamento disciplina ai sensi dell'articolo 4, comma 7 della L. 219/2017 la raccolta di copia delle dichiarazione anticipate di trattamento, compresa l'indicazione del fiduciario e il loro inserimento nella banca dati, ed al contempo attua l'articolo 1 della l.r. 13/2006, che stabilisce, che la Regione Toscana debba disciplinare con proprio regolamento il trattamento dei dati sensibili;

2. Si stabilisce che titolari del trattamento dei dati sono la Regione Toscana, per quanto attiene alle attività di gestione, archiviazione, conservazione, governo monitoraggio e controllo delle DAT, e le aziende sanitarie, la Fondazione Monasterio ed ISPRO, per quanto attiene alle attività di raccolta e utilizzo delle stesse;

3. Si dispone, inoltre, che le operazioni eseguibili dai soggetti autorizzati sono la raccolta, registrazione, modifica, sostituzione e revoca, consultazione e conservazione;

4. Si precisa, inoltre, che fino a che non verrà realizzata la banca dati nazionale ai sensi dell'articolo 1, commi 418 e 419 della legge 205/2017, le DAT potranno essere consultate, nel momento in cui il loro paziente non sia più in grado di autodeterminarsi, dai medici iscritti al servizio sanitario regionale;

5. Al fine di consentire la rapida attuazione delle disposizioni legislative, è necessario disporre l'entrata in vigore il giorno successivo alla pubblicazione sul Bollettino ufficiale della Regione Toscana.

Approva il presente regolamento

Art. 1
Oggetto e finalità

1. Il presente regolamento disciplina, ai sensi dell'articolo 4, comma 7 della legge 22 dicembre 2017, n. 219 (Norme in materia di consenso informato e di disposizioni anticipate di trattamento), la raccolta di copia delle dichiarazioni anticipate di trattamento (DAT) da parte delle aziende sanitarie, della Fondazione Monasterio e di ISPRO o dell'indicazione dove esse siano conservate e del fiduciario, se indicato, nonché i tipi di dati trattati, le operazioni eseguibili, i soggetti che possono trattare i dati medesimi, le misure per la sicurezza dei dati, al fine di garantire la gestione

delle medesime DAT, nonché la loro fruibilità da parte dei medici, nel momento in cui abbiano in cura l’assistito e lo stesso non sia in grado di autodeterminarsi.

2. Il presente regolamento ha le seguenti finalità:

a) consentire la raccolta delle DAT presso le aziende sanitarie, la Fondazione Monasterio e ISPRO;

b) consentire le modalità di gestione, archiviazione e conservazione delle DAT all’interno del basamento informativo predisposto dalla Regione Toscana;

c) rendere fruibili le DAT ai medici nel momento in cui abbiano in cura il paziente che non sia in grado di autodeterminarsi;

d) consentire alla Regione Toscana le attività di governo, monitoraggio e controllo della raccolta delle DAT per dare piena attuazione a quanto previsto dalla l. 219/2017;

e) consentire il raccordo con la banca dati nazionale di cui all’articolo 1, comma 418 della legge 27 dicembre 2017, n. 205 (Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020), con i contenuti e le modalità che saranno previsti dal decreto ministeriale di cui al comma 419 del medesimo articolo.

Art. 2
Definizioni

1. Ai fini del presente regolamento si applicano le definizioni di cui all’articolo 4 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).

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

a) banca dati regionale DAT, l'applicativo unico regionale per la raccolta, l'archiviazione, la conservazione e la gestione delle DAT;

b) banca dati nazionale DAT, l'applicativo unico nazionale per la raccolta, l'archiviazione, la conservazione e la gestione delle DAT;

c) codice univoco regionale, il codice assegnato, attraverso una procedura automatica, ad ogni assistito a partire dal codice fiscale, tale da non consentirne l’identificazione diretta durante il trattamento dei dati personali;

d) credenziali di autenticazione, i codici e i dispositivi in possesso dell’interessato o di una persona autorizzata al trattamento dei dati personali, da questi conosciuti o ad essi univocamente correlati, utilizzati per l'autenticazione informatica;

e) disponente, la persona maggiorenne e capace di intendere e di volere, che in previsione di un’eventuale futura incapacità di autodeterminarsi, dopo aver acquisito adeguate informazioni mediche sulle conseguenze delle sue scelte, rilascia la DAT;

Art. 3

Disposizioni anticipate di trattamento

1. Le DAT sono lo strumento attraverso il quale ogni persona maggiorenne e capace di intendere e di volere, in previsione di una eventuale futura incapacità di autodeterminarsi e dopo aver acquisito adeguate informazioni mediche sulle conseguenze delle sue scelte, può esprimere le proprie volontà in materia di trattamenti sanitari nonché il consenso o il rifiuto rispetto ad accertamenti diagnostici o scelte terapeutiche o a singoli trattamenti sanitari.

2. Nelle DAT può essere fornita anche l'indicazione del fiduciario, individuato dalla stessa persona che ha redatto le DAT.

3. Il disponente può individuare un fiduciario supplente che lo rappresenti nel caso in cui il primo fiduciario risulti irreperibile.

4. Le DAT sono redatte in forma scritta su qualsiasi formato o nel formato predisposto dalla Regione Toscana.

5. Nel caso in cui le condizioni fisiche del paziente non lo consentano, le DAT possono essere espresse attraverso videoregistrazione o per mezzo di altri dispositivi che consentono alla persona con disabilità di comunicare secondo le modalità di cui all'articolo 6.

6. Le informazioni contenute nelle DAT sono da ritenersi categorie particolari di dati personali come definite all'articolo 9, comma 1 del reg. (UE) 679/2016.

Art. 4
Titolare del trattamento dei dati

1. La titolarità del trattamento è articolata tra le aziende sanitarie, la Fondazione Monasterio, ISPRO e la Regione Toscana, secondo quanto di seguito specificato:

a) contitolari del trattamento dei dati personali afferenti alla raccolta e l'utilizzo delle DAT sono le aziende sanitarie, la Fondazione Monasterio ed ISPRO;

b) titolare del trattamento per la gestione, l'archiviazione e la conservazione delle DAT nella infrastruttura informatica è la Regione Toscana;

c) titolare del trattamento per le attività di governo, monitoraggio e controllo, sulla base dei dati privati degli elementi identificativi diretti, è la Regione Toscana.

Art. 5
Tipi di dati personali

1. Per il perseguimento delle finalità di cui all'articolo 1, comma 2, lettere a), b), c) ed e) i titolari del trattamento delle DAT trattano anche le particolari categorie di dati di cui all'articolo 9, comma 1 del reg. (UE) 679/2016 nella misura in cui questi dati siano contenuti nelle dichiarazioni espresse dal disponente.

2. I dati personali sono raccolti in modo che siano adeguati, pertinenti e limitati rispetto alle finalità di cui all'articolo 1, comma 2.

3. I dati strettamente necessari alla raccolta delle DAT sono i seguenti: numero del documento di identità o di riconoscimento, nome, cognome, codice fiscale, luogo e data di nascita, sesso, cittadinanza, indirizzo di residenza, indirizzo email e dichiarazione del disponente che è stato adeguatamente informato da un medico.

4. Sono raccolti i medesimi dati relativi al fiduciario, oltre al suo recapito telefonico, che possono essere forniti dal disponente o dal fiduciario stesso.

5. Le DAT, firmate dal disponente, possono essere consegnate o trasmesse alle aziende sanitarie, alla Fondazione Monasterio e a ISPRO con le modalità indicate nel disciplinare tecnico di cui all'allegato A.

6. Gli operatori aziendali, che raccolgono le dichiarazioni, operano in qualità di pubblico ufficiale ed accedono opportunamente abilitati e profilati ad una applicazione web dedicata e, ove necessario, provvedono ad attestare la conformità delle copie per immagine dei documenti analogici secondo le modalità previste dal decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) (CAD).

7. Il titolare del trattamento della banca dati regionale DAT archivia i dati nel rispetto di misure di sicurezza tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio secondo le modalità individuate nel disciplinare tecnico di cui all'allegato A.

Art. 6
DAT videoregistrate o prodotte da altri dispositivi

1. Nel caso in cui le condizioni fisiche del paziente non consentano la redazione e la consegna delle DAT, le stesse possono essere espresse mediante videoregistrazione o con l’utilizzo di dispositivi che consentano alla persona con disabilità di comunicare, alla presenza di testimoni o di pubblici ufficiali secondo le previsioni normative che regolamentano l’autenticità di un atto.

2. Nel caso di cui al comma 1 le DAT possono essere consegnate o trasmesse da un soggetto, debitamente identificato, diverso dal disponente che lo rappresenta ai sensi di legge.

Art. 7
Operazioni eseguibili

1. Le operazioni relative alle DAT che possono essere svolte dai soggetti autorizzati, secondo le rispettive specifiche competenze, delle aziende sanitarie, della Fondazione Monasterio e di ISPRO sono le seguenti:

a)raccolta e registrazione;
b)modifica e sostituzione;
c)revoca;
d)raccolta dell'accettazione e della rinuncia del fiduciario;
e)registrazione del luogo di conservazione della DAT;
f)consultazione;
g)conservazione.

Art. 8

Raccolta e registrazione

1. A seguito della consegna o trasmissione della DAT, l’operatore registra i dati identificativi, di cui all’articolo 5, commi 3 e 4, del disponente e, se nominato, del fiduciario e, nei casi di cui all'articolo 6, del soggetto consegnatario diverso dal disponente.

2. L’operatore genera un codice univoco regionale composto dal codice fiscale del disponente, dalla data di rilascio e da un numero progressivo, il codice univoco regionale, che viene associato alla DAT.

3. Nel caso di documento cartaceo, che viene acquisito al sistema mediante scannerizzazione, il codice univoco regionale viene stampato su etichetta autoadesiva da apporre al documento che viene reso al disponente.

4. Nel caso di trasmissione attraverso l’apposita applicazione web dedicata, il sistema genera automaticamente il codice univoco regionale relativo alla DAT caricata dal disponente.

5. Nel caso di trasmissione via posta elettronica certificata (PEC), al mittente viene trasmessa allo, stesso indirizzo PEC, copia della DAT ed il codice univoco regionale generato.

6. Le DAT vengono archiviate, a seguito di scannerizzazione se cartacee ovvero acquisendo il documento informatico pervenuto a mezzo PEC.

Art. 9
Modifica e sostituzione

1. La modifica delle DAT richiede la sostituzione integrale delle stesse.

2. La sostituzione delle DAT comporta l’integrale perdita di effetti delle DAT precedentemente rese ed avviene con le stesse modalità del rilascio indicate nel disciplinare tecnico di cui all'allegato A. Le DAT sostituite vengono conservate con la modalità e per i tempi previsti dalle normative vigenti in materia di conservazione documentale.

Art. 10
Revoca

1. Il disponente revoca le DAT con le stesse modalità del rilascio previste dal disciplinare tecnico di cui all'allegato A. L’operatore ricerca sul sistema le DAT raccolte e procede alla revoca. Le DAT revocate non sono più disponibili nella banca dati e vengono conservate con la modalità e per i tempi previsti dalle normative vigenti in materia di conservazione documentale.

Art. 11
Raccolta dell'accettazione e della rinuncia del fiduciario

1. L’accettazione del fiduciario avviene con le modalità indicate nel disciplinare tecnico di cui all'allegato A.

2. Al fiduciario viene rilasciata una copia delle DAT.

3. Il fiduciario può rinunciare alla nomina con le stesse modalità con le quali l'ha accettata. Tale rinuncia viene comunicata al disponente.

4. Il disponente può revocare il fiduciario con le stesse modalità con le quali lo ha individuato.

Art. 12
Registrazione del luogo di conservazione delle DAT

1. Il disponente può non consegnare copia delle proprie DAT, indicando, tuttavia, dove esse siano reperibili. L’operatore registra le informazioni ricevute e ne rilascia una attestazione contenente i dati forniti ed il codice univoco regionale di cui all’articolo 8.

Art. 13
Consultazione

1. Le DAT in corso di validità sono consultabili dal medico che ha in cura il disponente, qualora quest’ultimo si trovi nell’incapacità di autodeterminarsi, a seguito di esplicita dichiarazione del medico stesso.

2. Il disponente può consultare le proprie DAT in corso di validità nonché quelle revocate con le modalità indicate nel disciplinare tecnico di cui all'allegato A.

Art. 14
Conservazione

1. Le DAT vengono conservate con le modalità e per i tempi previsti dalle normative vigenti in materia di conservazione documentale.

Art. 15
Accesso alla banca dati DAT

1. I dati personali contenuti nella banca dati regionale DAT sono trattati in modo lecito, corretto e trasparente, nel rispetto dei principi di cui alla normativa vigente in materia di protezione dei dati personali, soltanto dal personale appositamente autorizzato e istruito da ciascun contitolare del trattamento e sottoposto a regole di condotta analoghe al segreto professionale stabilite dallo stesso, qualora non sia tenuto per legge al segreto professionale.

2. I soggetti di cui al comma 1 accedono ai dati personali contenuti nella banca dati regionale DAT, secondo modalità e logiche di elaborazione strettamente funzionali ai compiti attribuiti a ciascuno di essi secondo quanto descritto nel disciplinare tecnico di cui all'allegato A.

3. La Regione Toscana, per le finalità di cui all’articolo 1, comma 2, lettera d), tratta i dati anagrafici relativi ai disponenti che hanno consegnato la DAT in modalità di pseudonimizzazione, privati degli elementi identificativi diretti, così come descritte nel disciplinare tecnico di cui all'allegato A.

4. Il sistema gestisce un’opportuna profilazione rendendo disponibili determinate funzionalità relative al profilo autenticato come precisato nel disciplinare tecnico di cui all'allegato A.

5. Gli operatori di sportello operano per conto delle aziende sanitarie, della Fondazione Monasterio e di ISPRO con funzione di addetti alla raccolta o gestione delle DAT.

6. I medici possono consultare le DAT, con le modalità indicate nel disciplinare tecnico di cui all'allegato A, soltanto nel caso in cui abbiano in cura il disponente e che lo stesso si trovi nell'incapacità di autodeterminarsi.

7. Ogni accesso alle DAT è registrato al fine di consentire al disponente di risalire all'identità dell'utente che ha acceduto alle DAT, la data e l'ora di accesso.

Art. 16
Diffusione dei dati

1. La diffusione dei dati personali e delle DAT è vietata.

Art. 17
Attività di governo, monitoraggio e controllo

1. La Regione Toscana, quale titolare del trattamento della banca dati regionale DAT, per il perseguimento delle finalità di cui all'articolo 1, comma 2, lettera d), tratta i dati privati degli elementi identificativi diretti e può procedere, anche mediante pubblicazione, alla diffusione degli stessi purché in forma esclusivamente anonima.

Art. 18
Misure di sicurezza

1. La sicurezza dei dati trattati dalla banca dati regionale DAT deve essere garantita in tutte le fasi del trattamento dei dati stessi, 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.

2. Il titolare del trattamento della banca dati regionale DAT adotta pertanto le modalità tecniche e le misure di sicurezza determinate ai sensi dell'articolo 32 del reg. (UE) 679/2016, così come specificate nel disciplinare tecnico di cui all'allegato A.

Art. 19
Codifica dei dati trattati

1. Le categorie particolari di dati personali di cui all'articolo 9, comma 1 del reg. (UE) 679/2016 contenuti nella banca dati regionale DAT, 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 inintelliggibili 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 alla banca dati regionale DAT 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. 20
Informativa agli interessati

1. Ciascun contitolare del trattamento della banca dati DAT deve fornire l’informativa agli interessati, redatta ai sensi dell’articolo 13 del reg. (UE) 679/2016, ed è tenuto a garantire agli interessati il pieno e tempestivo esercizio dei diritti previsti all’articolo 15 del suddetto regolamento con le modalità previste nel disciplinare tecnico di cui all'allegato A.

2. L’informativa deve, tra l’altro, evidenziare che:

a) il medico che accede alle DAT dell’assistito non ha certezza che le DAT che consulta presso la banca dati del servizio sanitario regionale toscano siano effettivamente le ultime rilasciate dal disponente in quanto dalla suddetta banca dati non possono risultare eventuali DAT rilasciate successivamente ai notai, ai comuni o al sistema sanitario di altre regioni;

b) non sono presenti nella banca dati le DAT già rilasciate ai notai e comuni, a meno che queste non siano state consegnate dallo stesso disponente anche presso le aziende sanitarie.

Art. 21
Comunicazione in merito agli incidenti informatici

1. Sono comunicate all’Autorità Garante per la protezione dei dati personali, entro settantadue ore dalla conoscenza del fatto, le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali oggetto di trattamento per la tenuta e il funzionamento della banca dati regionale DAT ai sensi dell’articolo 33 del regolamento (UE) 679/2016, con le modalità previste nel disciplinare tecnico di cui all'allegato A.

2. Il titolare del trattamento comunica all'interessato, senza giustificato ritardo, la violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Art. 22
Disposizione transitoria

1. Nelle more della realizzazione di condizioni di interoperabilità tra le regioni, le disposizioni relative alla fruibilità delle DAT ai medici, nel momento in cui abbiano in cura il paziente che non sia in grado di autodeterminarsi, sono riferite ai medici del servizio sanitario regionale.

Art. 23
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 e ulteriori disposizioni di dettaglio

Introduzione

La Regione Toscana, al fine di regolamentare la raccolta e la fruizione delle disposizioni anticipate di trattamento (DAT), intende creare un basamento informativo regionale dedicato come punto unico di archiviazione digitale delle DAT. La Regione intende, inoltre, fornire uno strumento per la redazione e la raccolta delle DAT presso le strutture sanitarie: si tratta di una funzionalità ad hoc per la gestione di questa base dati, che viene aggiunta ad un applicativo web già in uso presso gli sportelli ASL per la gestione dei consensi del Fascicolo Sanitario Elettronico (FSE). La sezione aggiuntiva è denominata ‘Gestione DAT’, l'applicativo sarà di seguito indicato come GPF DAT.

Il basamento informativo (SIS DAT) e l'applicativo GPF DAT rappresentano il sistema regionale di gestione DAT.

La Regione Toscana ha inoltre definito un modulo cartaceo unico a livello regionale per la redazione delle DAT predisposto per la lettura ottica.

Riferimenti normativi

- ❒Legge 219 del 22 Dicembre 2017 – articolo 4, comma 7

Attori del sistema

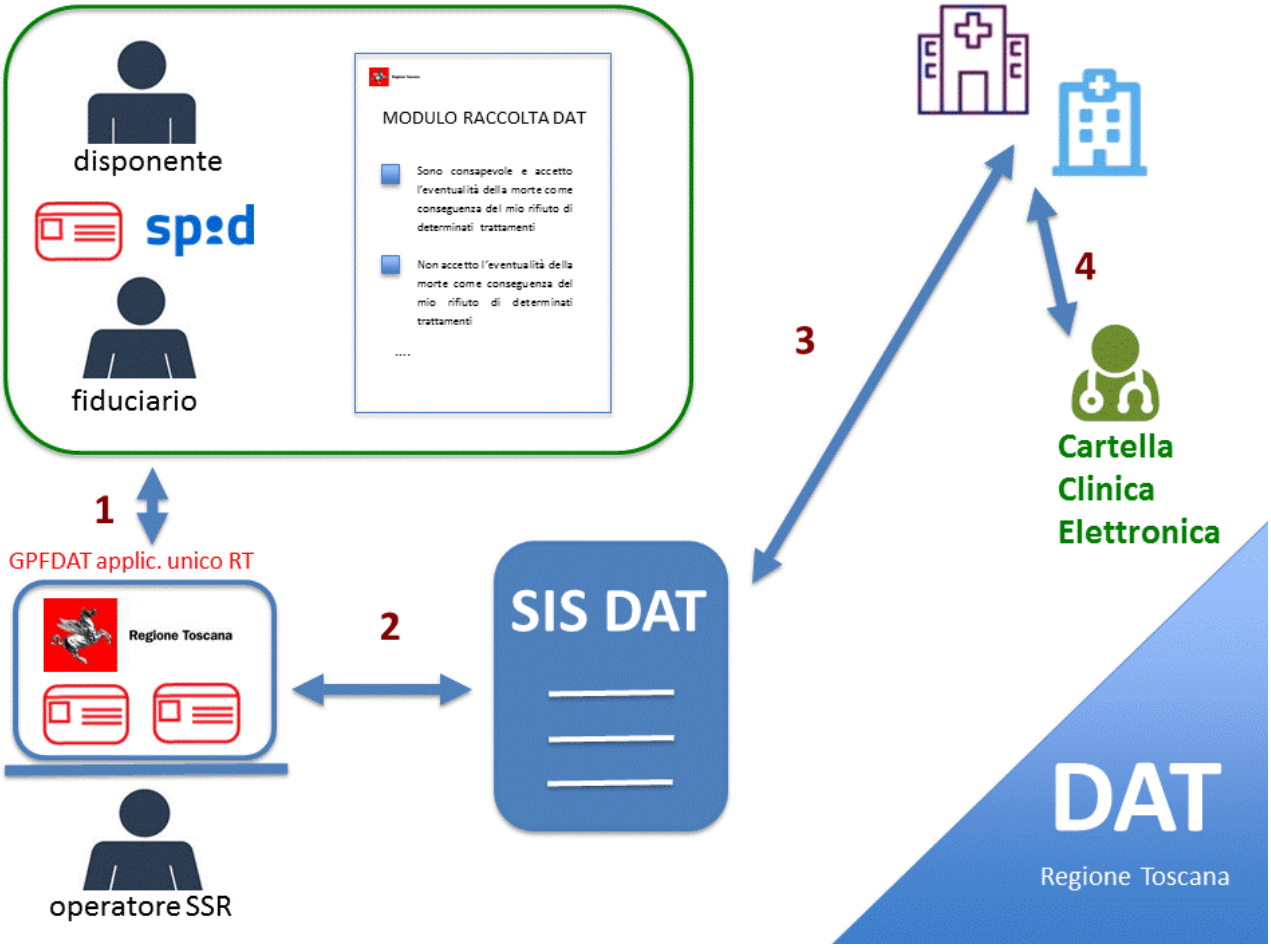
Gli attori che interagiscono con il sistema di gestione DAT sono i seguenti:

✓disponente

✓fiduciario

✓operatori e medici autorizzati presso strutture SSR

Flusso gestione DAT



2. Assets tecnologici

I sistemi devono presentare una intrinseca sicurezza rispetto al trattamento dei dati come richiesto dal GDPR e più in generale una realizzazione di codice di qualità. Il sistema a supporto della gestione delle DAT è parte del sistema sanitario regionale come il Fascicolo Sanitario Elettronico da cui mutua l'architettura e l'organizzazione.

3. Accesso e autorizzazione

L'accesso al sistema Informativo Regionale (SIR) della Regione Toscana avviene tramite la Carta Nazionale dei Servizi (CNS), il Sistema Pubblico di Identità Digitale (SPID) o altra moda modalità prevista da Regolamento eIDAS e della quale è dichiarata la conformità con il GDPR nel registro dei trattamenti del Titolare. Trattandosi di trattamento di dati di terzi il sistema richiede il livello SPID 3 per gli operatori abilitati.

Il SIR ha il compito di:

1.consentire all'utente di accedere ai dati in modo controllato applicando le regole stabilite dalla profilazione della applicazione e quelle relative al consenso;

2.gestire il tracciamento degli accessi, che comprende:

1.il tracciamento dell'identità dell'utente che ha accesso alla applicazione, la data e l'ora di accesso e una informazione che indica l'utente che ha effettuato l'accesso

2.il tracciamento delle operazioni svolte. In particolare si tiene traccia, all'interno di opportune tabelle di log, di informazioni relative al tipo di operazione svolta (servizio invocato), data e ora dell'operazione, identificazione dell'utente che svolge l'operazione, esito, oltre a informazioni per la misura della qualità del servizio.

3.1 Amministratori di sistema

Una diversa profilazione a livello di sistema di persistenza garantisce che gli utenti autorizzati all'accesso ai dati personali non possano accedere agli atri dati del sistema e viceversa. Questa caratteristica è definita a livello organizzativo e sono tracciati i permessi con una rendicontazione periodica delle abilitazioni.

Per ciascun utente è garantito l'accesso nominale strettamente personale ad ogni componente sia sistematica che applicativa per la quale è abilitato.

3.2 Sistema di pseudonimizzazione

Il sistema di pseudonimizzazione dei dati consiste nella separazione dei contenuti anagrafici dagli altri a livello di memorizzazione (persistenza) e di gestione (infrastruttura e organizzazione).

I sistemi, per essere conformi a questo standard regionale, non devono contenere al proprio interno informazioni anagrafiche strutturate, le uniche informazioni anagrafiche sono conservate nel

sistema di Circolarità anagrafica che attribuisce a ciascuna anagrafica un identificativo univoco pseudo-casuale per ciascun ambito del SIR. Cioè l'identificativo per il Sottosistema Sanità è diverso da quello del Sottosistema Lavoro.

Tramite questo processo i dati sensibili, relativi ai vari trattamenti, vengono archiviati senza riferimento ai dati personali del soggetto, ed il legame con il soggetto a cui si riferiscono, è mantenuto tramite l'identificativo del soggetto presente nel componente di Circolarità anagrafica.

La pseudonimizzazione prevede che il soggetto venga identificato in modalità sufficientemente forte mediante CNS, SPID o, più in generale, quanto previsto da Regolamento eIDAS.

Il processo di pseudonimizzazione si applica in tutti i contesti in cui è necessario persistere dati aggiuntivi oltre ai dati personali identificativi del soggetto.

Il sistema che riceve i dati procede alla pseudonimizzazione che è realizzata all'ingresso dei dati nel SIR e comunque il prima possibile rispetto al processo di gestione. Tutte le attività successive sono svolte implementando la ricomposizione solo quando è strettamente necessaria e limitando la persistenza alla sola esportazione di contenuti in modalità per le quali non sia possibile mantenere la pseudonimizzazione, come ad esempio nel caso della generazione di un documento autoconsistente, tipicamente un certificato in formato PDF.

In altri termini i dati personali sono persistiti su sistemi distinti da quelli che persistono gli altri dati tramite l'utilizzo di Motori di persistenza fisicamente distinti. Questa separazione avviene anche a livello di gruppi operativi che gestiscono il sistema (Amministratori).

3.3 Separazione

Il sistema di pseudonimizzazione è il cardine della separazione e del confinamento dei dati, insieme con l'adozione di misure di separazione dei ruoli, non solo mediante la gestione separata dei permessi, e prevede:

1.la separazione logica dei sistemi dell'infrastruttura in due gruppi distinti di macchine, garantendo che su ciascuno di essi possano essere conservati su file di database o di log esclusivamente dati di tipo anagrafico o dati non anagrafici pseudonimizzati o anonimizzati. In nessun caso i due insiemi di dati possono essere archiviati sullo stesso sistema (il trattamento congiunto dei due tipi di dati è ammesso esclusivamente nella memoria volatile);

2.due gruppi distinti di amministratori dei sistemi e delle basi di dati, aventi un accesso limitatamente all'uno o all'altro dei due gruppi di macchine sopra descritti.

Viene gestita la definizione di profili di autorizzazione agli amministratori dei sistemi di elaborazione e di persistenza, mediante la politica precedentemente descritta di separazione in due gruppi distinti di sistemi e di amministratori, ciascuno di essi aventi diritto ad operare con massimi privilegi esclusivamente sui dati anagrafici o sui dati pseudonimizzati.

Tali profili sono costruiti per garantire:

1.l'esecuzione di attività di tipo sistemistico mediante account nominali (eliminando pertanto l'esigenza di utilizzare account sistemistici di gruppo se non per casi limitati di emergenza opportunamente registrati);

2.la possibilità di svolgere attività amministrative solo nell’ambito dei sistemi che trattano le tipologie di informazioni per le quali l’operatore di sistema è stato preventivamente autorizzato, nell’ottica della separazione dei ruoli;

3.la possibilità di svolgere limitate attività di natura sistemistica (quali ad esempio il riavvio del sistema o lo start/stop dei servizi) sui sistemi sui quali l’operatore non è autorizzato ad accedere alle informazioni.

3.4 Crittografia

Ove la Separazione e la pseudonimizzazione non sono applicabili con costi e rischi accettabili, si pensi ad esempio a un PDF firmato da conservare in persistenza, si ricorre alla crittografia. Si ricorre alla crittografia anche in tutti quei casi in cui è necessario ridurre ulteriormente il rischio.

La crittografia dei dati residenti sui sistemi di persistenza è effettuata a livello software dallo storage o dal motore DB onde evitare la possibilità di estrarre direttamente informazioni dai file di database, qualora esportati su sistemi diversi.

3.5 Procedura di gestione

Sono attivate le seguenti procedure:

1.procedure di verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli amministratori dell’infrastruttura, con gestione centralizzata dei profili amministrativi;

2.tracciamento degli accessi ai sistemi ed alle basi di dati dell’infrastruttura, i quali avvengono (secondo procedure ordinarie) mediante credenziali assegnate in modo nominale al personale autorizzato;

3.procedure periodiche di verifica della effettiva separazione organizzativa fra amministratori dei sistemi di circolarità anagrafica e altri amministratori.

Tale tracciamento è effettuato utilizzando i log dei sistemi e delle basi di dati, acquisito in tempo reale da un’infrastruttura di log management dedicata in grado di assicurare l’integrità e la protezione contro accessi non autorizzati delle informazioni raccolte.

Il tracciamento prevede altresì la registrazione delle operazioni (incluso l’esito) svolte utilizzando privilegi di tipo amministrativo mediante account nominali.

In caso di operazioni rilevanti sotto il profilo della sicurezza, quali ad esempio l’accesso mediante credenziali amministrative di gruppo o la creazione di nuovi account sui sistemi, oltre al tracciamento è previsto un meccanismo di alerting via email utilizzando una casella di posta la cui gestione non è attribuita al personale che svolge attività sistemistica sull’infrastruttura.

Tutti i dati raccolti confluiscono infine in report di sintesi, generati automaticamente con frequenza mensile, a disposizione dei responsabili del servizio e/o di eventuali auditor.

3.6 Procedura di emergenza

La procedura di emergenza è in grado di assicurare la possibilità di ripristino dell'operatività dei sistemi in caso di incidenti, quando l'uso di account amministrativi di gruppo sia necessario.

In tali casi gli operatori di sistema possono fare richiesta ed ottenere tempestivamente tali credenziali (diverse per ogni account/sistema) scrivendo in un apposito registro il periodo e le motivazioni di utilizzo di tali account. La gestione separata degli account amministrativi assicura che, al termine dell'utilizzo di tali utenze, la password sia cambiata e resa sconosciuta agli addetti alla gestione dell'infrastruttura. L'utilizzo del registro in caso di assegnazione delle credenziali garantisce un adeguato livello di tracciamento. Ogni attività effettuata in emergenza deve essere descritta e resa verificabile mediante l'apertura e la chiusura di un "ticket" su un sistema di change management.

3.7 Gestione applicativa

Le applicazioni e le componenti applicative sviluppate per le funzioni di gestione delle DAT sono consegnate a livello di codice sorgente e verificate in fase di consegna in ambiente di staging. A seguito di verifica/collaudo viene disposto il passaggio in produzione.

Il codice è consegnato su una piattaforma di continuous integration (QMSS) per la verifica della qualità statica dello stesso e la correzione di segnalazioni prima dell'avvio in produzione. La risoluzione delle evidenze consente di migliorare la qualità abbattendo il rischio di errori funzionali.

Tutte le comunicazioni fra sottosistemi avvengono mediante canali protetti a livello di rete e resi sicuri dalla crittografia e/o dalla gestione di livello di firewalling diversificati e stratificati.

Il team di sviluppo non dispone delle credenziali di accesso ai sistemi e ai database in quanto tali informazioni sono residenti sui sistemi e vengono utilizzate dalla infrastrutture che ospitano l'applicazione e non direttamente dall'applicazione stessa.

3.8 Procedure Data Breach

Nel caso in cui dati trattati subiscano violazioni tali da comportare la perdita, la distruzione o la diffusione indebita di dati personali, il titolare del trattamento consulta tempestivamente il responsabile della protezione dei dati (RPD). Nei casi previsti dal regolamento UE 2016/679, deve essere effettua una segnalazione al Garante per la protezione dei dati personali, entro 72 ore dal momento in cui il Titolare è venuto a conoscenza dell'evento, contenente quanto previsto dal comma 3 dell'articolo 33 del regolamento UE 2016/679.

Il titolare del trattamento comunica all'interessato, senza giustificato ritardo, la violazione dei dati personali suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

MODALITA’ CON LE QUALI LE DISPOSIZIONI VENGONO RESE ALLE AZIENDE

a) Le DAT che non prevedono l’individuazione del fiduciario:

- consegnate, anche in copia, personalmente dal disponente, previa identificazione, presso specifici sportelli individuati dalle aziende sanitarie, dalla Fondazione Monasterio e da ISPRO;

- trasmesse dal disponente attraverso apposita applicazione web dedicata che consente la trasmissione delle stesse, con allegate copie di documento di riconoscimento e del codice fiscale;

- trasmesse dal disponente a mezzo di PEC all’indirizzo di PEC dedicato, con allegate copie di documento di riconoscimento e del codice fiscale;

b) Le DAT che prevedono l’individuazione del fiduciario, firmate dal disponente e dal fiduciario per accettazione, possono essere:

- consegnate, anche in copia, personalmente dal disponente, previa identificazione, presso specifici sportelli individuati dalle aziende sanitarie, dalla Fondazione Monasterio e da ISPRO, allegando copia del documento di identità e del codice fiscale del fiduciario.;

- trasmesse dal disponente attraverso apposita applicazione web dedicata che consente la trasmissione delle stesse, con allegate copie di documento di riconoscimento e del codice fiscale del fiduciario;

- trasmesse dal disponente a mezzo di PEC all’indirizzo di PEC dedicato, con allegate copie di documento di riconoscimento e del codice fiscale, allegando inoltre copia del documento di identità e del codice fiscale del fiduciario per accettazione.

c) Le DAT che prevedono l’individuazione del fiduciario, firmate dal solo disponente a cui spetta l’onere di informare il fiduciario sugli adempimenti di cui al successivo punto d) e di dichiarare che il fiduciario ha autorizzato lo stesso disponente a fornire i suoi dati personali:

- consegnate, anche in copia, personalmente dal disponente presso specifici sportelli individuati dalle Aziende sanitarie, dalla Fondazione Monasterio e da ISPRO;

- trasmesse dal disponente attraverso apposita applicazione web dedicata che consente la trasmissione delle stesse, con allegate copie di documento di riconoscimento e del codice fiscale;

- trasmesse dal disponente a mezzo di PEC all’indirizzo di PEC dedicato, con allegate copie di documento di riconoscimento e del codice fiscale.

d) nel caso di cui al punto c), l’accettazione successiva firmata dal fiduciario - che deve riportare il nome del disponente e il codice univoco regionale rilasciato al disponente - viene:

- consegnata personalmente dal fiduciario presso gli sportelli;

- trasmessa dal fiduciario a mezzo di PEC all’indirizzo di PEC dedicato, allegando copia del documento di identità e del codice fiscale;

e) le medesime modalità previste per l’individuazione e l’accettazione del fiduciario valgono per il fiduciario supplente di cui all’articolo 3, comma 3.

PROCEDURE PER L’ACCESSO ALLA BANCA DATI SIS DAT

a) L'accesso del personale autorizzato avviene tramite autenticazione mediante Carta nazionale dei servizi di cui all'articolo 66, comma 2 del CAD o credenziali del sistema pubblico di identità digitale (SPID) di livello 3 di cui all'articolo 64 del CAD, (oltre al nome utente e la password è necessario un supporto fisico, ad esempio una “smart card” per l'identificazione) sia per la raccolta da parte degli operatori che per la consultazione da parte del personale medico.

b) L’accesso al sistema per la consultazione da parte del disponente avviene tramite le credenziali SPID almeno di livello 2 (nome utente e una password scelti dall'utente, più la generazione di un codice temporaneo di accesso “one time password”).