Decreto del Presidente della Giunta Regionale 9 luglio 2012, n. 55/R

Regolamento di attuazione dell' articolo 76 bis, comma 8, legge regionale 24 febbraio 2005, n. 40 (Disciplina del servizio sanitario regionale) in merito all'istituzione del Fascicolo Sanitario Elettronico. ***(1)***

(Bollettino Ufficiale n. 54, parte prima, del 15.10.2012)

INDICE

PREAMBOLO
Art. 1 - Oggetto del regolamento (articolo 76 bis, comma 8, l. r. 40/2005)
Art. 2 - Destinatari (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 3 - Accesso al FSE (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 4 - Consenso (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 5 - Formazione e implementazione del FSE (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 6 - Dati soggetti a tutela dell'anonimato (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 7 - Soggetti del SSR e dei servizi socio-sanitari abilitati alla formazione e implementazione del FSE (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 8 - Dati e documenti che confluiscono nel FSE (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 9 - Profilo sanitario sintetico "patient summary" (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 10 - Taccuino personale del cittadino (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 11 - Accesso in emergenza (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 12 - Operazioni eseguibili (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 13 - Modalità del trattamento dei dati (articolo 76 bis, comma 8, l.r. 40/2005)
Art. 14 - Disattivazione del fascicolo in caso di decesso dell'assistito (articolo 76 bis, comma 8, l.r. 40/2005)
Allegato A - DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FASCICOLO SANITARIO ELETTRONICO (articolo 13 del regolamento).

Il PRESIDENTE DELLA GIUNTA

EMANA

il seguente regolamento

PREAMBOLO

Visto l'articolo 117, comma 6 della Costituzione;

Visto l'articolo 42, comma 2 dello Statuto della Regione Toscana

Vista la legge regionale 24 febbraio 2005, n 40 (Disciplina del servizio sanitario regionale), articolo 76 bis;

Viste le "Linee guida in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario" approvate dall'Autorità Garante per la protezione dei dati personali il 16 luglio 2009;

Viste le "Linee guida sul fascicolo sanitario elettronico" proposte dal Ministero della Salute ed approvate in Conferenza Stato-Regioni il 10 febbraio 2011;

Visto il parere del Comitato tecnico di direzione espresso nella seduta del 24 maggio 2012;

Visto il parere della Direzione generale della Presidenza;

Vista la deliberazione di Giunta regionale 30 luglio 2012, n. 701;

Visto il parere della Commissione consiliare competente, espresso nella seduta del 5 settembre 2012;

Considerato che l'articolo 76 bis, comma 8, l.r. 40/2005 dispone che con atto di natura regolamentare si individuano i dati e i documenti che confluiscono nel FSE, le operazioni eseguibili, i soggetti del Servizio Sanitario Regionale che aderiscono al sistema provvedendo alla formazione ed implementazione del fascicolo stesso, nonché le modalità organizzative di espressione del consenso;

Vista la deliberazione della Giunta regionale 24 settembre 2012, n. 842;

si approva il presente regolamento

Art. 1
Oggetto del regolamento (articolo 76 bis, comma 8, l. r. 40/2005)

1. Il presente regolamento, in attuazione dell'articolo 76 bis, comma 8, della legge regionale 24 febbraio 2005 n 40, (Disciplina del servizio sanitario regionale) individua i dati e i documenti sanitari e socio-sanitari che confluiscono nel fascicolo sanitario elettronico (FSE), le operazioni eseguibili, i soggetti del servizio sanitario regionale (SSR) e dei servizi socio-sanitari che aderiscono al sistema provvedendo alla formazione ed implementazione del FSE, nonché le modalità organizzative di espressione del consenso.

Art. 2
Destinatari (articolo 76 bis, comma 8, l.r. 40/2005)

1. Usufruiscono del FSE tutti gli assistiti dalle aziende sanitarie della Regione Toscana, per i quali sia prevista dalla normativa vigente l'emissione della tessera sanitaria-carta nazionale dei servizi (TS-CNS), di cui all'articolo 11, comma 15 del decreto legge 31 maggio 2010, n. 78 (Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica) convertito con Legge 30 luglio 2010, n. 122.

Art. 3
Accesso al FSE (articolo 76 bis, comma 8, l.r. 40/2005)

1. Lo strumento per l'accesso dell'assistito al proprio FSE è la CNS, dotata di un codice di accesso personale e segreto.

2. Il FSE è uno strumento a disposizione dell'interessato, che può decidere di farlo consultare ai professionisti e agli operatori sanitari.

3. Nei casi di emergenza sanitaria o di igiene pubblica, rischio grave, imminente e irreparabile per la salute e l'incolumità fisica dell'interessato, i medici del SSR possono accedere al FSE secondo le modalità specificate nell'articolo 11.

4. Ogni accesso alle informazioni contenute nel FSE è registrato in apposita sezione a disposizione dell'interessato.

Art. 4
Consenso (articolo 76 bis, comma 8, l.r. 40/2005)

1. Il FSE può essere attivato solo dopo che l'assistito ha preso visione dell'informativa relativa al trattamento dei dati inseriti nel FSE ed ha espresso un esplicito consenso alla sua attivazione.

2. Il consenso all'attivazione del FSE può essere espresso presso uno dei punti di attivazione individuati, oppure per via telematica previa attivazione e autenticazione tramite TS-CNS.

3. Nel caso di minore o di persona sottoposta a tutela, il consenso deve essere espresso dal tutore, mediante l'esibizione di un proprio documento di identità. In caso di attivazione telematica il consenso deve essere espresso dal tutore, che ha provveduto all'attivazione della TS-CNS del minore o del tutelato mediante esibizione di un proprio documento di identità.

4. Al raggiungimento della maggiore età, il consenso deve essere confermato da un'espressa manifestazione di volontà del neo-maggiorenne, dopo aver preso visione dell'informativa, recandosi ad uno dei punti di attivazione. Qualora il consenso non sia confermato esplicitamente, il FSE viene disattivato dopo tre mesi dal raggiungimento della maggiore età, in maniera equivalente ad una esplicita operazione di revoca del consenso, di cui al comma 6.

5. Nei casi in cui l'interessato sia impossibilitato per motivi di salute ad attivare personalmente il proprio FSE, lo stesso può delegare all'attivazione un altro soggetto, che deve produrre una delega sottoscritta dal delegante accompagnata dalla copia di un documento di identità dello stesso e un proprio documento d'identità.

6. L'interessato può in ogni momento revocare, con accesso telematico o tramite dichiarazione resa presso uno dei punti di attivazione, il consenso prestato in precedenza.

7. La revoca di cui al comma 6 determina l'interruzione dell'alimentazione del FSE e la disabilitazione dell'accesso, senza conseguenze in ordine all'erogazione delle prestazioni del SSR e dei servizi socio-sanitari. Il FSE viene comunque alimentato da eventuali correzioni dei dati che lo hanno composto fino alla revoca del consenso, da parte degli organismi sanitari che hanno generato tali dati.

8. In caso di successiva riattivazione vengono resi nuovamente visibili nel FSE i dati che lo hanno implementato fino alla precedente operazione di revoca, ivi comprese le correzioni anche successive alla revoca del consenso.

9. Una volta disattivato, il FSE resta disponibile in conformità agli obblighi di legge per 10 anni.

10. Il consenso all'attivazione del FSE vale anche quale consenso per l'accesso al proprio FSE da parte di professionisti ed operatori sanitari nei casi di emergenza sanitaria o igiene pubblica, rischio grave, imminente e irreparabile per la salute e l'incolumità fisica dell'interessato, secondo le modalità specificate nell'articolo 11.

11. All'interessato deve essere garantita la possibilità di esercitare, in ogni momento, i diritti di cui all'articolo 7 del decreto legislativo 30 giugno 2003,n. 196 (Codice in materia di protezione dei dati personali) nei confronti dei dati personali trattati nel FSE. Tali diritti sono esercitati direttamente nei confronti dei titolari del trattamento, che possono dare riscontro alle richieste dell'interessato mediante annotazione delle modifiche, senza alterazione della documentazione di riferimento.

12. All'interessato devono inoltre essere garantite facili modalità di consultazione del proprio FSE.

Art. 5

Formazione e implementazione del FSE (articolo 76 bis, comma 8, l.r. 40/2005)

1. Una volta prestato il consenso alla sua attivazione, e ad eccezione dei dati disciplinati da disposizioni normative a maggior tutela dell'anonimato, l'assistito può decidere se il suo FSE sia alimentato in maniera automatica, per cui tutti i dati e i documenti sanitari e socio-sanitari vi confluiscono automaticamente, oppure in maniera selettiva, alimentando il proprio FSE per ogni singolo dato e documento sanitario e socio-sanitario o per classi di essi, tramite una sezione separata del fascicolo in cui vengono mostrate le sole informazioni di sintesi e non il suo dettaglio. L'assistito può variare la modalità di alimentazione in qualsiasi momento.

2. L'assistito ha il diritto di oscurare dal FSE dati e documenti sanitari e socio-sanitari che lo hanno precedentemente alimentato; in questo caso i dati e i documenti sanitari e socio-sanitari oscurati vengono mantenuti in una sezione separata del FSE con le sole informazioni di sintesi e non il loro dettaglio; i dati e i documenti sanitari e socio-sanitari oscurati possono comunque essere nuovamente inseriti fra i contenuti del FSE.

Art. 6

Dati soggetti a tutela dell'anonimato (articolo 76 bis, comma 8, l.r. 40/2005)

1. I dati e i documenti sanitari e socio-sanitari disciplinati da disposizioni normative a maggiore tutela dell'anonimato, in particolare quelle a tutela delle vittime di atti di violenza sessuale o di pedofilia, delle persone sieropositive, di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che si sottopongono a un'interruzione volontaria di gravidanza o che decidono di partorire in anonimato, nonché con riferimento ai servizi offerti dai consultori familiari, possono essere resi visibili solo previo esplicito consenso dell'interessato, ferma restando la possibilità per l'assistito di ricorrere alla prestazione in anonimato, che rende impossibile da parte dei soggetti che erogano le prestazioni l'alimentazione del FSE.

2 E' responsabilità dei professionisti o degli operatori sanitari che erogano la prestazione acquisire l'esplicito consenso dell'interessato.

Art. 7

Soggetti del SSR e dei servizi sociosanitari abilitati alla formazione e implementazione del FSE (articolo 76 bis, comma 8, l.r. 40/2005)

1. I soggetti che nello svolgimento della loro attività professionale nell'ambito di un processo di cura alimentano in maniera continuativa il FSE sono:

a) aziende sanitarie;

b) i medici di medicina generale e pediatri di libera scelta, inclusi i loro sostituti e coloro che esercitano in forma associata;

c) ogni altro soggetto, anche privato, che operi all'interno del SSR e dei servizi socio-sanitari.

2. La titolarità del trattamento dei dati personali è dell'esercente la professione sanitaria o dell'organismo

socio sanitario presso cui sono redatte le informazioni sanitarie che alimentano il FSE.

3. Ciascuna categoria di titolari di cui al comma 1 può accedere alle informazioni sanitarie che ha prodotto, anche ai fini di verificarne la correttezza su segnalazione dell'interessato.

Art. 8

Dati e documenti che confluiscono nel FSE (articolo 76 bis, comma 8, l.r. 40/2005)

1. Il FSE è costituito da un indice che lega i dati personali dell'interessato a tutte le prestazioni che lo riguardano e che garantisce la visibilità delle stesse. I dati personali sono composti dai dati anagrafici contenuti nell'anagrafe regionale degli assistiti e dalle informazioni amministrative relative alla posizione dell'interessato nei confronti del SSR e dei servizi socio-sanitari.

2. Il FSE si alimenta a partire dalla data in cui l'assistito esprime per la prima volta il proprio consenso alla sua attivazione. Fanno eccezione i dati relativi ad esenzioni per patologia e vaccinazioni per le quali viene mostrato il dato attivo o in corso di validità.

3. I dati e documenti sanitari e socio-sanitari, rilasciati da soggetti del SSR e dei servizi socio-sanitari, sono tutti quelli che riguardano l'assistito nel suo percorso all'interno del SSR, tra i quali:

a) referti;
b) accessi e verbali di pronto soccorso;
c) lettere di dimissioni;
d) schede di dimissione ospedaliera;
e) registri operatori;
f) assistenza domiciliare;
g) assistenza residenziale e semiresidenziale;
h) profilo sanitario sintetico "patient summary";
i) bilanci di salute;
j) erogazione farmaci;
k) prescrizioni farmaceutiche;
l) vaccinazioni;
m) certificati.

4. I dati anagrafici, conservati separatamente dai dati idonei a rivelare lo stato di salute in applicazione dell'articolo 22, comma 7, d.lgs.n.196/2003 sono ricongiungibili, al momento dell'accesso ai dati stessi da parte di un utente autorizzato, ai dati e documenti sanitari e socio-sanitari tramite la funzione di gestione dell'indice, di cui è titolare del trattamento la Regione.

5. L'indice contiene anche le informazioni sul consenso che l'assistito ha espresso relativamente all'attivazione del FSE e alla visibilità delle prestazioni ivi contenute.

Art. 9

Profilo sanitario sintetico "patient summary" (articolo 76 bis, comma 8, l.r. 40/2005)

1. Il profilo sanitario sintetico "patient summary", è il documento socio sanitario informatico redatto e aggiornato dal medico di medicina generale/pediatra di libera scelta, che riassume la storia clinica del paziente e la sua situazione corrente.

2. La finalità del profilo sanitario sintetico "patient summary" è di favorire la continuità di cura, permettendo un rapido inquadramento del paziente al momento di un contatto non previsto, come in caso di emergenza e pronto soccorso.

3. I dati essenziali che compongono il profilo sanitario sintetico "patient summary" sono riconducibili a quelli individuati nelle "Linee guida nazionali - Il fascicolo sanitario elettronico", di cui all'intesa tra Governo, Regioni e Province autonome del 10 febbraio 2011, ai sensi dell'articolo 8, comma 6, della legge 5 giugno 2003, n. 131 (Disposizioni per l'adeguamento dell'ordinamento della Repubblica alla L.Cost. 18 ottobre 2001, n. 34).

4. La titolarità del trattamento dei dati contenuti nel profilo sanitario sintetico "patient summary" è del medico di medicina generale e pediatra di libera scelta, che procede alla redazione dello stesso. 5. Nell'ambito del FSE, il medico di medicina generale/pediatra di libera scelta rende disponibile il profilo sanitario sintetico "patient summary" tramite l'azienda sanitaria con la quale è in rapporto di convenzione, al fine di alimentare il FSE, e per i soli cittadini che lo hanno attivato.

Art. 10

Taccuino personale del cittadino (articolo 76 bis, comma 8, l.r. 40/2005)

1. Nell'ambito del FSE è prevista una sezione riservata all'interessato denominata "taccuino personale del cittadino" che vi può inserire dati e informazioni personali, file di documenti sanitari, un diario di

eventi rilevanti, promemoria per i controlli medici periodici.

2. Le informazioni e i documenti inseriti nel taccuino personale del cittadino risultano dati non certificati.

3. I dati e documenti con cui l'assistito alimenta questa sezione del FSE vengono resi disponibili tramite l'azienda sanitaria di iscrizione.

Art. 11

Accesso in emergenza (articolo 76 bis, comma 8, l.r. 40/2005)

1. Nei casi di emergenza sanitaria o igiene pubblica, rischio grave, imminente e irreparabile per la salute e l'incolumità fisica dell'interessato, i medici del SSR e dei servizi socio-sanitari, utilizzando la propria TS-CNS/Carta Operatore, possono accedere al FSE dell'interessato.

2. Lo stato di emergenza di cui al comma 1 è esplicitamente dichiarato e sottoscritto dal medico del SSR e le sue dichiarazioni e gli accessi ai dati sono memorizzati in maniera tale che l'interessato possa verificarli, consultando il suo FSE.

3. In tali situazioni le informazioni del FSE che possono essere consultate sono quelle rese visibili dall'assistito, secondo le modalità di cui al precedente articolo 6.

Art. 12

Operazioni eseguibili (articolo 76 bis, comma 8, l.r. 40/2005)

1. Sui dati personali e documenti sanitari e socio-sanitari contenuti nel FSE possono essere effettuate operazioni di registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, interconnessione, blocco, cancellazione e distruzione, da parte di ciascun titolare sui dati di propria competenza.

2. I dati di cui al comma 1 non possono essere oggetto di comunicazione a terzi da parte del titolare, salvo nei casi in cui sia necessario per ottemperare ad obblighi di legge o di regolamento.

3. Per lo svolgimento delle operazioni di conservazione dei dati e documenti sanitari e socio-sanitari e di alimentazione dell'indice, i titolari possono avvalersi dell'attività di fornitori di servizi, espressamente individuati quali responsabili esterni del trattamento dei dati.

Art. 13

Modalità del trattamento dei dati (articolo 76 bis, comma 8, l.r. 40/2005)

1. I dati personali e i dati e documenti sanitari e socio-sanitari dell'interessato contenuti nel FSE sono memorizzati, distribuiti e indicizzati all'interno di una apposita infrastruttura tecnologica per la gestione del FSE, sono trattati attraverso strumenti elettronici e sono trasmessi attraverso reti telematiche.

2. Ciascun titolare assicura che ogni operazione su tali dati avviene con un livello di sicurezza elevato ed adotta tutte le misure di sicurezza dei dati e dei sistemi che sono individuate nel disciplinare tecnico, contenuto nell'Allegato A), al presente regolamento.

3. Il disciplinare tecnico di cui al comma 2 è integrato ed aggiornato in relazione all'evoluzione tecnologica.

Art. 14

Disattivazione del fascicolo in caso di decesso dell'assistito (articolo 76 bis, comma 8, l.r. 40/2005)

1. Al momento del decesso dell'assistito, il suo fascicolo viene disattivato: ciò determina la disabilitazione dell'accesso. Il fascicolo viene comunque alimentato da eventuali correzioni dei dati che lo hanno composto fino alla disattivazione, da parte degli organismi sanitari che hanno generato tali dati.

2. Il FSE viene conservato per eventuali obblighi di legge per 10 anni.

Allegato A

DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FASCICOLO SANITARIO ELETTRONICO (articolo 13 del regolamento).

Ferme restando le misure di sicurezza, individuate negli articoli da 31 a 36 del Decreto Legislativo 30 giugno 2003 n. 196 e nel Disciplinare Tecnico pubblicato in Allegato B) a tale Decreto, il presente Disciplinare dispone le misure di sicurezza specifiche per la gestione il Fascicolo sanitario elettronico .

La sicurezza dei dati trattati nel FSE deve essere assicurata in tutte le fasi del trattamento dei dati, adottando opportuni accorgimenti che preservino i medesimi dati da rischi di accesso abusivo, furto o smarrimento degli stessi.

Tutte le operazioni di seguito indicate sono svolte da incaricati appositamente individuati ed edotti in materia di protezione dei dati personali nonché sui profili di rischio che incombono sui dati.

Sulla base delle linee guida sul FSE da parte del Garante per la Privacy e del regolamento di attuazione del comma 8, articolo 76 bis (Fascicolo Sanitario Elettronico) sono stati attivati i seguenti meccanismi per la tutela della privacy sul contenuto informativo relativo ai cittadini:

- Il sistema di anonimizzazione dei dati descrive la modalità di comunicazione e archiviazione delle informazioni sanitarie e anagrafiche.

Nell'ambito del Sistema Informativo Socio Sanitario di Regione Toscana, nel caso in cui l'Azienda sanitaria non sia in grado di inviare la prestazione già anonimizzata, l'anonimizzazione viene effettuata da componenti software sviluppate dalla Regione e installate sui sistemi di cooperazione applicativa nel dominio Aziendale;

Tramite questo processo i dati sensibili, relativi a prestazioni sanitarie, 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 nell'anagrafe regionale (iduniversale).

Il processo di anonimizzazione si applica in tutti i contesti in cui i dati sanitari sono legati ai dati personali identificativi del soggetto.

Questi gli ambiti di applicazione del processo di anonimizzazione nel contesto regionale:

• Anonimizzazione di prestazioni comunicate a Flussi (es. specialistica ambulatoriale, ricoveri,farmaceutica,ecc);

• Anonimizzazione di prestazioni comunicate a Eventi – RFC (es. Pronto Soccorso, Laboratorio,ecc);

• Anonimizzazione di prestazioni comunicate tramite Applicazioni (es. caricamento dati pregressi degli eventi di RSA).

I soggetti presenti nel record di ogni singola prestazione, possono essere identificati da più tipologie di codice in funzione del tipo di prestazione. Sono infatti previsti:

• codice fiscale

• codice Sanitario

• codice STP

• tessera sanitaria TEAM

L'anonimizzazione prevede quindi che l'identificazione del soggetto possa avvenire a partire da uno degli identificativi sopra elencati.

La gestione del consenso nel Fascicolo Sanitario Elettronico avviene su livelli diversi:

• il cittadino deve inizialmente esprimere un consenso affinché i suoi dati possano essere raccolti per gli scopi del Fascicolo Sanitario. Finché il cittadino non esprime il consenso, i dati sulle prestazioni sanitarie non sono raccolti. Analogamente i dati non vengono raccolti se il consenso viene negato;

• nel caso in cui sia espresso un consenso positivo alla raccolta dei dati, il cittadino è poi chiamato a concedere o negare il consenso su ogni singola prestazione o gruppi di prestazioni. Solo le prestazioni per cui è stato acquisito un consenso positivo potranno essere mostrate nel FSE.

Di seguito viene data la descrizione degli scenari e delle scelte operative che si riferiscono alla gestione del consenso per il sistema regionale della Toscana, di gestione delle prestazioni sanitarie e, in particolare, al sistema di consultazione di FSE.

Un evento prestazionale è un messaggio XML che trasporta informazioni su una prestazione erogata o su un evento rilevante dal punto di vista amministrativo o sanitario. Il messaggio è inviato dalle Aziende Sanitarie erogatrici della prestazione al CART e ricevuto (secondo le regole stabilite per il dominio applicativo) dai soggetti titolati a trattare tali informazioni.

Lo scenario di cooperazione secondo cui un sistema informativo Aziendale comunica informazioni su prestazioni sanitarie prevede tipicamente le seguenti interazioni:

1. il sistema informativo della ASL invia gli eventi prestazionali verso il NAL Aziendale;
2. un componente applicativo installato sul NAL inoltra l'evento sull'infrastruttura CART dopo averlo validato e anonimizzato;
3. il Sottosistema Regionale di Sottoscrizione e Archiviazione su TIX riceve gli eventi da CART e svolge le seguenti prestazioni:

• recupera il codice identificativo del cittadino a cui la prestazione si riferisce;

• controlla se il cittadino ha dato il consenso per la attivazione del fascicolo sanitario elettronico;

• nel caso in cui il cittadino abbia dato il consenso, inserisce i dati della prestazione negli Archivi Prestazionali Aziendali del TIX, che contengono le prestazioni erogate da ognuna delle Aziende Sanitarie/Ospedaliere toscane.

Una volta che l'informazione sulla prestazione è stata inserita all'interno degli archivi aziendali, può essere messa a disposizione del Fascicolo.

In particolare per ogni prestazione potrà essere presente la seguente informazione di consenso:

• il codice identificativo dell'assistito;

• il codice della prestazione;

• la data di espressione del consenso;

• il tipo di consenso espresso (es. consenso concesso/negato)

Le prestazioni per le quali il consenso non è concesso o per le quali non esiste alcuna informazione di consenso (perché il consenso non è stato espresso dall'assistito) non sono mostrate in Fascicolo Sanitario. Un consenso non espresso viene quindi considerato equivalente ad un consenso negato.

- L'accesso al Fascicolo Sanitario Elettronico di Regione Toscana avviene tramite la Carta Nazionale dei Servizi (CNS).

Il riconoscimento dell'utente avviene tramite il portale di autenticazione ARPA, che realizza una infrastruttura di servizi di autenticazione e autorizzazione, parte integrante del nodo regionale del Sistema Pubblico di Connettività.

L'applicazione che gestisce il Fascicolo Sanitario, ha il compito di:

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

• gestire il tracciamento degli accessi.

Questo in particolare comprende:

- o il tracciamento dell'identità dell'utente che ha accesso alla applicazione, la data e l'ora di accesso e una informazione che indica se l'utente che ha effettuato l'accesso è l'assistito stesso o un soggetto diverso (ad esempio un medico di emergenza- urgenza);
- o il tracciamento delle operazioni svolte relativamente al consenso. In particolare si tiene traccia, all'interno di opportune tabelle di log, di informazioni relative al tipo di operazione svolta (es. concessione/revoca del consenso), data e ora dell'operazione, identificazione dell'utente che svolge l'operazione.

In entrambi i casi, la base di dati consente solo di effettuare inserimenti all'interno delle tabelle di log e non aggiornamenti o cancellazioni.

Il sistema dei dati personali. Nella realizzazione del FSE, come parte integrante del sistema, sono state stabilite le seguenti regole:

• il sistema prevede profili diversi per i soggetti che trattano dati sensibili o personali per il tramite della separazione dei dati in DB distinti;

• le informazioni sensibili (es. dati prestazionali), vengono raccolte sulla base dati in forma anonimizzata.

Inoltre, in ottemperanza a quanto previsto dalle linee guida FSE del Garante, sono realizzate anche le seguenti misure di sicurezza:

- la cifratura di tutti i dati di natura sensibile residenti sui DBMS con chiavi distinte per le informazioni sanitarie e per gli assistiti a cui le informazioni stesse fanno riferimento. Tali chiavi sono gestite da personale diverso da coloro che hanno accesso ai sistemi per attività di gestione, onde evitare la possibilità di estrarre direttamente informazioni dai file di database, qualora esportati su sistemi diversi. Le chiavi, distinte per tipologia di informazione, sono assegnate a persone diverse, in modo da evitare che la decifratura di un set di informazioni consenta la ricostruzione completa del dato personale sensibile attribuito ad uno specifico assistito Interessato;

- l'adozione di misure di separazione dei ruoli, non solo mediante la gestione separata delle chiavi crittografiche precedentemente descritta, prevedendo:

a) 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 sanitari in forma anonima. In nessun caso i due insiemi di dati possono essere archiviati, anche temporaneamente, sullo stesso sistema (il trattamento congiunto dei due tipi di dati è ammesso esclusivamente nella memoria volatile);

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

- limitazione dell'accesso sistemistico all'infrastruttura che gestisce dati sanitari, tramite un sistema "ponte" le cui credenziali sono a conoscenza esclusivamente del personale autorizzato;

- limitazione dell'accesso sistemistico all'infrastruttura da remoto, mediante meccanismi di virtual private network su canale cifrato;

- accesso nominale da parte di tutti gli operatori che svolgono attività di tipo sistemistico, sia sui sistemi operativi che sui DBMS dell'infrastruttura;

- segregazione delle credenziali amministrative di gruppo (ad esempio root, Administrator, etc...), le quali

sono poste sotto la custodia di personale non coinvolto nella gestione sistemistica dell'infrastruttura e che non ha la possibilità di accedere ai sistemi non disponendo dell'accesso alla macchina "ponte".

- definizione di profili di autorizzazione agli amministratori dei sistemi e dei database, 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 anonimi di natura sanitaria. Tali profili sono costruiti per garantire:
  a) 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);
  b) 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;
  c) 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;
  d) la possibilità di consentire la gestione degli applicativi impedendo tuttavia l'accesso ai dati di log che possono contenere i dati elaborati dai servizi.

I profili sono costruiti sulla base di "white list" di comandi autorizzati, negando pertanto ogni operazione che non sia stata preventivamente autorizzata;

- 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;

- come detto precedentemente, separazione logica e fisica (quando applicabile) dei sistemi che trattano i dati sensibili, garantendo che le informazioni sensibili siano conservate in modo separato dai dati identificativi degli assistiti a cui appartengono. Tali dati non si trovano mai (neppure su file temporanei) residenti sul medesimo disco (per "disco" si intende un volume logico accessibile da un singolo sistema), mentre la correlazione è mantenuta soltanto nell'ambito dell'elaborazione nella memoria volatile. I due gruppi di sistemi sono amministrati da gruppi di amministratori distinti;

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

- le procedure di emergenza in grado di assicurare la possibilità di ripristino dell'operatività dei sistemi in caso di incidenti, anche 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.

Note

1. A s*eguito dell'entrata in vigore della l.r. 28 dicembre 2015, n. 84, art. 93, il presente regolamento rimane in vigore limitatamente all'allegato A "Disciplinare tecnico in materia di misure di sicurezza per il fascicolo sanitario elettronico" per le disposizioni compatibili con il d.p.c.m. 178/2015 sino all'adozione della deliberazione di cui all'articolo 76 bis, comma 9 della l.r. 40/2005.*