

REGIONE TOSCANA

Direzione Generale Diritti di Cittadinanza e Coesione Sociale

DICHIARAZIONE DEI REDDITI PRECOMPILATA

...

Progetto Regionale per la trasmissione dei dati
delle spese mediche al Sistema TS

Versione 1.01

Servizio Accoglienza Regionale (SAR)

INDICE

Revisioni del documento.....	3
1. Premessa.....	4
2. Normativa di riferimento	4
3. Aspetti generali	4
3.1 scenario nazionale.....	4
3.2 modalità di trasmissione	5
3.3 monitoraggio stato attuazione	5
3.4 tracciato dati	6
4. Scenario Regione Toscana	8
4.1 tipologia dei dati inviati	8
4.2 linee progettuali	8
4.3 schema.....	9
5. Descrizione generale architetturale	10
5.1 RTRT.....	10
5.2 CART	10
5.3 RFC	10
5.4 icar.....	10
5.5 accesso ai servizi	10
5.6 anagrafe assistiti	10
6. Sicurezza dati e privacy	12
6.1 Sistema di anonimizzazione.....	12
6.2 Accessi	13
6.3 Cifratura.....	13
6.4 Procedure di emergenza.....	15

REVISIONI DEL DOCUMENTO

VERSIONE	PARAGRAFO	DATA MODIFICA	DESCRIZIONE
1.00		25.02.2015	Prima stesura
1.01		14.04.2015	Seconda stesura

1. PREMESSA

Il presente documento descrive le modalità ed il trattamento dei dati da trasmettere al sistema TS inerenti le spese sanitarie sostenute dal Cittadino, ai fini della precompilazione della dichiarazione dei redditi, secondo le modalità previste dalla normativa vigente.

2. NORMATIVA DI RIFERIMENTO

Articolo 50 - Legge 30 settembre 2003, n. 269, convertito con modificazioni dalla legge 24 novembre 2003, n. 326 e successive modifiche, relativi alle “Disposizioni in materia di monitoraggio della spesa nel settore sanitario e di appropriatezza delle prescrizioni sanitarie”. (Gazzetta Ufficiale n. 274 del 25 novembre 2003 - Supplemento Ordinario n. 181).

Articolo 3 - Decreto Legislativo 21 novembre 2014, n. 175. Trasmissione all'Agenzia delle entrate da parte di soggetti terzi di dati relativi a oneri e spese sostenute dai contribuenti:

- **Comma 2.** Ai fini della elaborazione della dichiarazione dei redditi, l'Agenzia delle entrate può utilizzare i dati di cui all'articolo 50, comma 7, del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326.
- **Comma 3.** Ai fini della elaborazione della dichiarazione dei redditi, le aziende sanitarie locali, le aziende ospedaliere, gli istituti di ricovero e cura a carattere scientifico, i policlinici universitari, le farmacie, pubbliche e private, i presidi di specialistica ambulatoriale, le strutture per l'erogazione delle prestazioni di assistenza protesica e di assistenza integrativa, gli altri presidi e strutture accreditati per l'erogazione dei servizi sanitari e gli iscritti all'Albo dei medici chirurghi e degli odontoiatri, inviano al Sistema tessera sanitaria, secondo le modalità previste dal decreto del Presidente del Consiglio dei ministri 26 marzo 2008, attuativo dell'articolo 50, comma 5-bis, del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, e successive modificazioni, i dati relativi alle prestazioni erogate nel 2015 ad esclusione di quelle già previste nel comma 2, ai fini della loro messa a disposizione dell'Agenzia delle entrate. Le specifiche tecniche e le modalità operative relative alla trasmissione telematica dei dati, sono rese disponibili sul sito internet del Sistema tessera sanitaria.

3. ASPETTI GENERALI

3.1
scenario
nazionale

Ai fini della predisposizione della dichiarazione dei redditi precompilata da parte dell'Agenzia delle Entrate di cui al D. Lgs. 175/2014, l'art. 3 comma 3 del medesimo DLgs 175/2014 prevede che il Sistema Tessera Sanitaria metta a disposizione dell'Agenzia delle entrate le informazioni concernenti le spese sanitarie sostenute dai cittadini nell'anno 2015, trasmesse telematicamente al medesimo Sistema dalle strutture sanitarie e dagli iscritti all'albo dei medici chirurghi e degli odontoiatri, secondo le modalità previste dal DPCM 26/3/2008.

A tal fine, si sono tenute due riunioni presso il Dipartimento RGS del MEF, in data 21

gennaio 2015 e 5 febbraio 2015, presenti i rappresentanti del Ministero della Salute, dell'Agenzia delle Entrate, della Regione Veneto per il Coordinamento della Commissione Salute e delle regioni Lombardia, Emilia Romagna, Toscana e Umbria, nonché di Sogei.

Nel corso delle riunioni si è convenuto quanto segue:

1. Art. 3, comma 2 del D.Lgs. 175/2014: Utilizzo dei dati già presenti nel Sistema Tessera Sanitaria (ex comma 5 dell'art. 50 del DL 269/2003).

Trattasi dei soli dati relativi al ticket delle prestazioni a carico del SSN di specialistica, inviate al Sistema Tessera Sanitaria ai sensi del comma 5 dell'art. 50 del DL 269/2003.

Al riguardo, le regioni hanno fatto presente alcune criticità relative all'utilizzo di tali dati da parte dell'Agenzia delle entrate per le finalità di cui al D. Lgs. 175/2014, in quanto tali dati non sempre contengono l'indicazione di effettivo pagamento del ticket e la data ("data di cassa"), risultante sulla fattura di pagamento del ticket.

Trattasi infatti di dato attualmente facoltativo del tracciato ex comma 5 dell'articolo 50, che le strutture di specialistica non sempre avvalorano, in quanto non interconnesse con i dati relativi alla cassa.

Inoltre, risultano casistiche per le quali il cittadino procede al pagamento del ticket ma non usufruisce della prestazione, chiedendo un rimborso del ticket pagato.

In tali termini, nel corso delle riunioni, è emersa la necessità di **attivare un nuovo flusso che attesti:**

- **l'effettivo ticket pagato e relativa data del pagamento;**
- **eventuale rimborso del ticket pagato.**

3.2
modalità di
trasmissione

Modalità di trasmissione

Restano ferme le modalità di trasmissione già previste dal Sistema TS:

- Abilitazioni alla trasmissione telematica: risultano valide le credenziali già attive per il collegamento telematico al Sistema TS, con la possibilità di collegare direttamente al Sistema TS tutti gli altri utenti responsabili dei nuovi flussi (Uffici delle ASL responsabili del pagamento del ticket, etc)
- Soggetti "delegati" ai sensi del comma 8 dell'art. 50
- Sistemi regionali (c.d. "comma 11")

3.3
monitoraggio
stato
attuazione

Monitoraggio stato di attuazione

Saranno resi disponibili dal portale del Sistema TS le necessarie reportistiche per consentire il puntuale rispetto degli adempimenti previsti a livello regionale per la trasmissione dei dati

Tracciato ministeriale dei dati

Nome campo	Descrizione	Caratteristiche	Controlli	Note
Data	Data di emissione del “documento fiscale” relativo alla spesa sostenuta dal cittadino.	<u>Elemento obbligatorio</u>	Scarto dei dati in caso di data futura rispetto alla data di trasmissione ovvero non conforme	Il campo data e idspesa costituiscono la chiave del record per variazioni, rimborsi e cancellazioni
Idspesa	Numero progressivo del “documento fiscale” relativo alla spesa sostenuta dal cittadino	<u>Elemento obbligatorio</u>	Formale e scarto in caso di non univocità del dato nell’ambito della fornitura.	Il campo data e idspesa costituiscono la chiave del record per variazioni, rimborsi e cancellazioni
Flag Operazione	Indica il tipo di operazione da eseguire sul record. Valori ammessi: “P” = inserimento ovvero nuovo record; “V” = Variazione “R” = Rimborso “C” = Cancellazione	<u>Elemento obbligatorio</u>	Scarto del dato in caso di difformità rispetto ai valori previsti	
Codice Fiscale Cittadino	Codice fiscale, del cittadino rilevato dalla Tessera Sanitaria, “crittografato” secondo le modalità di cui al decreto attuativo del comma 5 dell’articolo 50 del DL 269/2003	<u>Elemento obbligatorio</u>	Formali rispetto alle anagrafiche di riferimento del sistema TS	Scarto di tutto i dati in caso di non esistenza e non validità del CF
<u>Natura di spesa</u>	Indicare esclusivamente una delle seguenti tipologie di natura di spesa sostenuta dal cittadino. Il Campo assume i seguenti valori: • TF= Ticket (Quota fissa e/o Differenza con il prezzo di riferimento) • TS= Ticket (Franchigia e/o Quota fissa) • TP=Ticket pronto soccorso • TA=Ticket accesso diretto • FO= Farmaco, anche omeopatico • FV = Farmaco per uso veterinario • PG= Preparazioni galeniche • AD= Acquisto o affitto di dispositivo medico CE • AP = Affitto o acquisto di protesi. • AS= Spese sanitarie relative ad	<u>Elemento obbligatorio</u>	Scarto del dato in caso di difformità rispetto ai valori previsti	

Nome campo	Descrizione	Caratteristiche	Controlli	Note
	ECG, spirometria, Holter pressorio e cardiaco, test per glicemia, colesterolo e trigliceridi o misurazione della pressione sanguigna, prestazione previste dalla farmacia dei servizi e simili sanguigna) • SP= Spese prestazioni assistenza specialistica ambulatoriale esclusi interventi di chirurgia estetica. Visita medica generica e specialistica o prestazioni diagnostiche e strumentali. Prestazione chirurgica ad esclusione della chirurgia estetica • RO= Ricoveri ospedalieri • CT= Cure Termali • PI= protesica e integrativa (extra farmacia e strutture accreditate) • CM= Certificazione Medica • IC= Intervento di chirurgia estetica ambulatoriale o ospedaliero • AA= Altre spese			
<u>Importo</u>	Importo di ogni singola spesa sostenuta dal cittadino	Elemento obbligatorio	Formali	

4. SCENARIO REGIONE TOSCANA

Ai sensi del comma 11 dell'art. 50 del DL 269/2003 e dell'art. 4 del DPCM 26/3/2008, Regione Toscana ha realizzato un sistema di accoglienza regionale (SAR), dispiegato e pienamente operativo per la specialistica ambulatoriale, per la prescrizione elettronica e la ricetta dematerializzata, in grado di supportare tutti i processi ed i flussi indirizzati verso il servizio di accoglienza centrale (SAC).

In tale scenario, Regione Toscana chiede, per il debito informativo in oggetto, la trasmissione tramite il proprio Sistema di Accoglienza Regionale (SAR) ai sensi del comma 11 dell'art. 50 del DL 269/2003 e dell'art. 4 del DPCM 26/3/2008, limitatamente alle tipologie di spese sanitarie riportate nella terza colonna ("collegamento al Sistema TS tramite sistema regionale") della sottostante tabella :

4.1
tipologia dei
dati inviati

tipologie di spese sanitarie sostenute dai cittadini:	collegamento al Sistema TS		note	specificità regionali
	diretto con il Sistema TS	tramite sistema regionale		
a) Ticket per le prestazioni di specialistica, pronto soccorso, terme;				
a.1) prestazioni di specialistica		X		
a.2) pronto soccorso		X		
a.3) terme	X			
b) spese sanitarie sostenute dal cittadino per prestazioni erogate in regime di intramoenia;		X		
c) altre spese sanitarie sostenute dal cittadino per prestazioni erogate dalle strutture sanitarie private accreditate;	X			
d) spese sanitarie sostenute dal cittadino per prestazioni erogate da medici iscritti all'Ordine dei medici chirurghi e odontoiatri (**);	X			
e) rilevazione dei c.d. "scontrini parlanti" emessi dalle farmacie pubbliche e private;	X			

**** tale rilevazione riguarda i medici convenzionati con il SSN. Per gli altri medici iscritti all'Ordine è previsto il collegamento diretto al Sistema TS.**

4.2
linee
progettuali

Da quanto descritto fino ad ora si evince che la progettualità oggetto del presente documento si basa sui seguenti punti cardine : l'istituzione di un nuovo flusso; l'utilizzo del SAR per le spese sostenute all'interno delle Aziende Sanitarie (specialistiche, pronto soccorso e intramoenia); l'avvio di una prima fase di attuazione, comprensiva del recupero dell'attività pregressa; la gestione a regime.

Prima fase

Per le spese relative all'anno 2015, prevede due invii : il primo a settembre 2015 ed il secondo entro gennaio 2016. In questa fase, la trasmissione dati avverrà "a flusso".

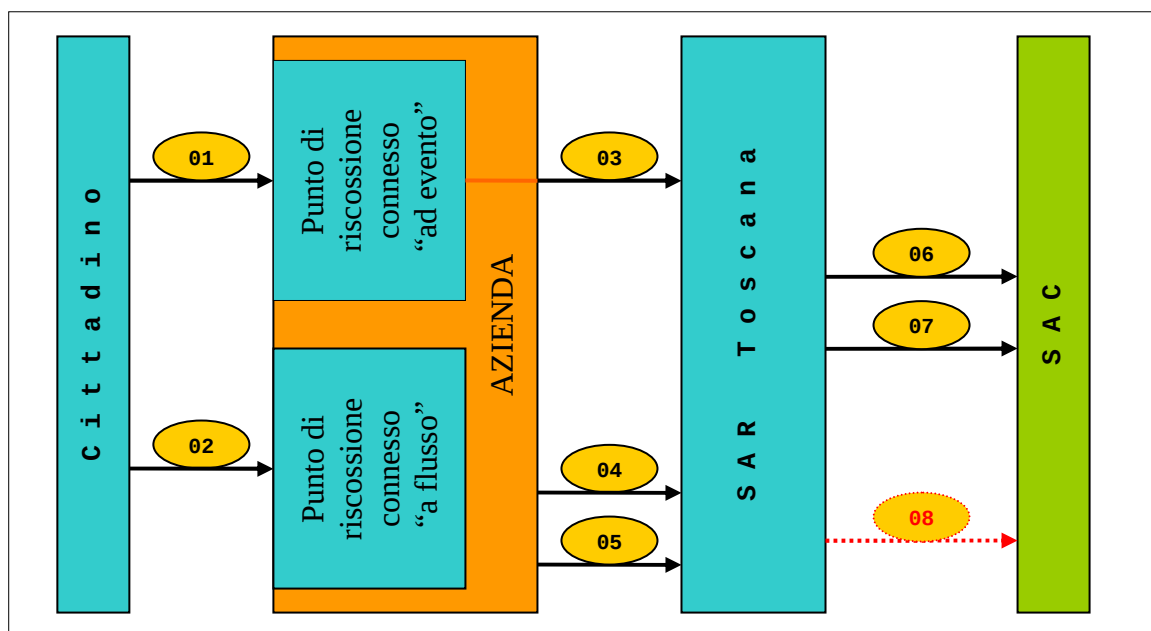
Fase a regime

Questo scenario prevede, in linea con lo sviluppo dei sistemi informativi regionali, l'invio dei dati in modalità "ad evento". Si prevede quindi la costituzione di un WS (web service) basato su RFC (Request For Comment) specifico.

I due scenari sopra descritti potranno convivere, tenuto conto della progressiva transizione di tutti i punti di riscossione coinvolti dalla prima alla seconda fase.

4.3
schema

Nello schema sotto riportato si evidenziano le transazioni principali che compongono l'intero processo. Tale schema rappresenta una semplificazione delle transazioni relative al processo oggetto del progetto, ma significative per identificare i canali principali di comunicazione.



01	Il Cittadino paga ad un punto di riscossione connesso "ad evento".
02	Il Cittadino paga ad un punto di riscossione connesso "a flusso".
03	Il "punto di riscossione" comunica in tempo reale il debito informativo al "SAR" tramite i sistemi informativi aziendali.
04	Il "punto di riscossione" comunica ai sistemi informativi della propria Azienda il debito informativo. L'azienda provvede ad inviare, con metodologia "a flusso", i dati presenti sui propri DB al SAR (invio di settembre).
05	Il "punto di riscossione" comunica ai sistemi informativi della propria Azienda il debito informativo. L'azienda provvede ad inviare, con metodologia "a flusso", i dati presenti sui propri DB al SAR (invio di gennaio).
06	Il SAR invia i dati al SAC con metodologia a flusso. Invio di Settembre.
07	Il SAR invia i dati al SAC con metodologia a flusso. Invio di Gennaio.
08	Ipotesi futura se il SAC predisporrà l'invio ad eventi. Il SAR invia in tempo reale i dati ricevuti dalle Aziende.

5. DESCRIZIONE GENERALE ARCHITETTURALE

Questa parte del documento descrive le infrastrutture regionali esistenti in grado di fornire servizi di connettività agli utenti ed alle Aziende Sanitarie e di interoperare con le infrastrutture di cooperazione applicativa del Sistema di Accoglienza Centrale (SAC), in attuazione dell'articolo 3, comma 1, del Decreto del Presidente del Consiglio dei Ministri, 26 marzo 2008, "Attuazione dell'articolo 1, comma 810, lettera c), della legge 27 dicembre 2006, n. 296, in materia di regole tecniche e trasmissione dati di natura sanitaria, nell'ambito del Sistema pubblico di connettività".

5.1
RTRT

La Rete Telematica Regionale Toscana è una rete di soggetti e una Infrastruttura Tecnologica diffusa su tutto il territorio regionale, interconnessa ad Internet, interoperante, in quanto rispondente agli standard promossi dal CNIPA (prima AIPA), con il Sistema Pubblico di Connettività.

In attuazione a tale legge LR 1/2004 gli enti pubblici utilizzano la Rete Telematica Regionale della Toscana.

La rete telematica prevede un centro servizi TIX (Tuscany Internet eXchange) dove i soggetti pubblici della Toscana possono disporre di servizi di qualità di housing e hosting, oltre che delle infrastrutture di sicurezza come backup, firewall, antivirus e quanto necessario a garantire misure minime richieste dalla CAD e dalla normativa in materia di Privacy. Il Centro servizi costituisce un NAP (Neutral Access Point) dove confluiscono Internet Service Provider (ISP) accreditati. Informazioni di dettaglio possono essere recuperate direttamente sul sito ufficiale del TIX <http://www.tix.it>.

5.2
CART

L'infrastruttura CART è lo strumento utilizzato dalle applicazioni interoperanti dei soggetti appartenenti alla comunità (Comunità e.Toscana) per scambiarsi informazioni. I punti fondamentali dell'architettura realizzata sono:

- l'aderenza ad un insieme di standard;
- l'uso dei servizi infrastrutturali.

L'infrastruttura CART è pienamente compatibile con le specifiche SPCoop emesse dal CNIPA e ne seguirà le evoluzioni. Il CART si sviluppa come una rete distribuita sul territorio regionale, costituita dai NAL (nodi locali ospitati negli Enti, in costante comunicazione con il CRIC (centro regionale di cooperazione), sia per permettere l'effettiva cooperazione tra i servizi applicativi ospitati nei Domini degli Enti, sia per permettere la gestione ed il monitoraggio centralizzati dei sistemi e dei processi di cooperazione in atto.

5.3
RFC

Le specifiche dei servizi erogati tramite Cart sono definite attraverso RFC (Request for Comment) che sono proposti dai soggetti interessati al Comitato Compliance di Regione Toscana al fine di ricevere la candidatura a diventare standard. Gli RFC rimangono candidati per un periodo di tempo in modo da consentire alla comunità di fare interventi e proporre o discutere eventuali miglioramenti. Essi vengono successivamente sottoposti all'approvazione del Comitato e.Toscana compliance per diventare standard di riferimento.

5.4
icar

Oltre alla integrazione a livello regionale è stata sviluppata un'altra iniziativa ICAR di livello nazionale: il progetto ICAR nasce dalla necessità di integrare sistemi informativi e gestionali in domini applicativi diversi e territorialmente distribuito. A questo progetto cofinanziato dai partecipanti e dalla Pubblica Amministrazione Centrale partecipano Tutte le Regioni e le Province autonome. Questo progetto produce Standard di comunicazione, accordi di servizio e software open source e riusabile che può essere integrato nei domini

Regionali e delle Province Autonome. In questo ambito la Toscana, in quanto capofila task INF 1, ha consegnato a tutti i soggetti ed attivato presso 15 di essi le Porte di Dominio (SPCoop). L'infrastruttura è quindi dispiegata su tutto il territorio nazionale.

L'infrastruttura CART è dunque aperta a tutte le infrastrutture che implementano gli standard SPCoop. Sul territorio regionale sono attualmente dispiegati 125 Nodi Applicativi Locali (NAL). Un NAL è un apparato hardware collocato presso un Ente le cui interfacce esposte tramite Proxy Applicativi consentono di inviare le informazioni ad un altro NAL e quindi ad un altro Ente.

Le norme di riferimento sono le seguenti :

- Decreto Legislativo 7 marzo 2005, n. 82 “Codice dell’amministrazione digitale”;
- Decreto Legislativo 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
- Legge 27 dicembre 2006, n. 296 “Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2007)”;
- Legge Regionale della Toscana 26 gennaio 2004, n. 1 “Promozione dell’amministrazione elettronica e della società dell’informazione e della conoscenza nel sistema regionale. Disciplina della Rete telematica regionale toscana”;
- Legge Regionale della Toscana n.40 del 2005;
- Legge Regionale della Toscana 5 ottobre 2009, n. 54 “Istituzione del sistema informativo e del sistema statistico regionale. Misure per il coordinamento delle infrastrutture e dei servizi per lo sviluppo della società dell’informazione e della conoscenza”.

5.5
accesso ai
servizi

L'accesso ai servizi di rete viene effettuato tramite infrastrutture ad alto grado di sicurezza ovvero standard CNS o da certificati applicativi rilasciati da una CA Regionale.

Oltre la Tessera Sanitaria, l’operatore del SSR ha come strumento di lavoro la “Carta dell’Operatore” (DGRT n. 7 del 2011 - Istituzione dell'anagrafe regionale degli operatori del Sistema Sanitario della Toscana e adozione della "Carta dell'Operatore"). Tale carta costituisce lo strumento per l’accesso alla rete e l’identificazione dell’operatore. La Carta dell’Operatore è corredata dal certificato di firma digitale per tutti gli operatori che necessitano di detta funzionalità.

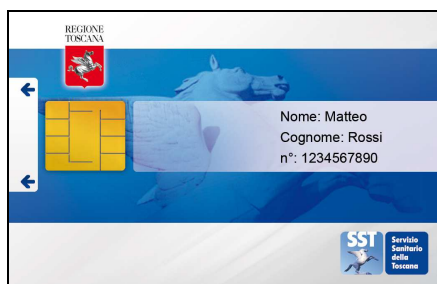


Figura 1 : Carta dell’ Operatore

Oltre a ciò Regione Toscana ha reso disponibile un sistema di single sign on basato su Autenticazione, determinazione del Ruolo, assegnazione del Profilo e Accesso. Tale infrastruttura consente l'autenticazione diretta o federata mediante protocolli aperti e sicuri SAML.

5.6
anagrafe
assistiti

L'anagrafe dei soggetti ha la finalità di consentire il riconoscimento dei cittadini in modo tale che le Aziende sanitarie possano identificarli in modo univoco in tutto il territorio

regionale e fuori da esso. Questo sottosistema si trova nel dominio di responsabilità della Regione.

Il sistema della prescrizione e certificazione è basato sul riconoscimento univoco delle persone a cui si riferiscono i dati. E' stato pertanto realizzato un sistema di circolarità anagrafica fra le Aziende Sanitarie e la Regione finalizzato al riconoscimento delle persone, all'associazione di un identificativo univoco non parlante e alla separazione dei dati personali da quelli sensibili come prescritto dal Codice in materia di protezione dei dati personali.

La circolarità anagrafica è realizzata mediante l'interazione di più sistemi. All'interno del Sistema Sanitario della Toscana le Aziende realizzano un'anagrafe centralizzata alla quale fanno riferimento i vari domini applicativi. Le applicazioni che afferiscono a ciascun dominio utilizzano come riferimento l'anagrafe unica aziendale che è sincronizzata in cooperazione applicativa con quella regionale. Ogni persona viene individuata con un identificativo univoco non parlante che è assegnato al momento del primo censimento. L'anagrafe regionale replica ogni variazione verso le anagrafi aziendali che a loro volta erogano servizi ai vari domini applicativi. L'anagrafe regionale è l'unica che interagisce con soggetti esterni al SST.

L'anagrafe regionale gestisce inoltre il livello di certificazione delle informazioni, in quanto informazione singole (es. codice fiscale) o gruppi di informazioni (es. residenza) hanno più fonti, a ciascuna delle quali è associata un livello di certificazione della fonte. Le informazioni possono essere aggiornate esclusivamente da fonti di rango equivalente o superiore. A titolo di esempio la residenza può essere auto-certificata, verificata da una ASL o certificata da un comune o dal Ministero degli Interni. L'autocertificazione non modifica la certificazione comunale, mentre è vero il contrario.

6. SICUREZZA DATI E PRIVACY

La sicurezza dei dati, ove previsto, 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.

Per garantire la sicurezza e la tutela della privacy sono stati attivati i meccanismi, evidenziati nei prossimi paragrafi, sul contenuto informativo relativo alla prescrizione.

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'inviante non sia in grado di inviare i dati già anonimizzati, 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 (id-universale).

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

6.1
Sistema di
anonimizzazione

- codice fiscale
- codice STP
- id-universale

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

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

1. il sistema informativo dell'inviante invia gli eventi prestazionali verso l'APS (Access Point Subsystem);
2. un componente applicativo installato sull' APS 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 li memorizza sul DB;
4. I dati validati vengono inviati al SAC.

6.2
Accessi

Il riconoscimento dell'utilizzatore del DB relativo ai dati archiviati avviene tramite una infrastruttura di servizi di autenticazione e autorizzazione, parte integrante del nodo regionale del Sistema Pubblico di Connettività.

L'applicazione che gestisce il DB, 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 e di gestire il tracciamento degli accessi.

6.3
Cifratura

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 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, prevede :

- 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.

Sono attivi anche i seguenti accorgimenti :

- 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.
- 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, 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;

6.4
*Procedure di
emergenza*

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.