Deliberazione della Giunta Regionale 10 gennaio 2012, n. 3-3259

Progetto "Realizzazione del Sistema di Anonimizzazione Reversibile del patrimonio informativo sanitario" - Approvazione del "Disciplinare delle modalita' di accesso al patrimonio informativo sanitario regionale e di esercizio della funzione di reversibilita' dei dati a fronte di qualificate esigenze" - Disposizioni organizzative in ordine all'istituzione della funzione di anonimizzazione.

A relazione degli Assessori Maccanti, Monferino:

Obiettivo strategico per l'Amministrazione regionale è promuovere lo sviluppo socio-economico del territorio piemontese anche attraverso l'utilizzo delle tecnologie dell'informazione e della comunicazione ICTs come leve strategiche per la pianificazione e realizzazione di iniziative volte alla completa inclusione digitale di cittadini, aziende e Pubbliche Amministrazioni e lo sviluppo di sistemi informativi idonei a sfruttare le potenziali sinergie derivanti dallo sviluppo integrato dei servizi erogati e fruibili sulla rete.

Con D.G.R. n. 9-5114 del 22 gennaio 2007 sono state approvate le "Linee guida del SIRE", quale documento descrittivo lo stato di attuazione della politica sostenuta dalla Regione Piemonte in materia di Società dell'Informazione, della Comunicazione e della Conoscenza, nonché base di pianificazione e realizzazione di nuove iniziative orientate alla completa "inclusione digitale" dei cittadini, aziende e PA.

Al fine di realizzare un sistema informativo integrato dell'intera Pubblica amministrazione (PA) piemontese, con deliberazione di Giunta regionale n. 41-6573 del 30 luglio 2007, è stato approvato il piano triennale per l'E-Government e la società dell'informazione in Piemonte, definendo i ruoli delle PA piemontesi ed il relativo piano di azione con le "Linee guida del piano di E-Goverment piemontese".

Con D.G.R. n. 15-8626 del 21 aprile 2008 la Giunta regionale ha poi approvato il "Programma SIRSE - Sistema Integrato Regionale di Sanità Elettronica" proponendo un modello di "sanità in rete" di cui le tecnologie ICT costituiscono fattore strategico per la realizzazione di nuovi modelli assistenziali, facilitando l'accesso alle informazioni cliniche da parte degli operatori sanitari e la fruizione di servizi da parte dei cittadini.

Con D.G.R. n. 24-11672 del 29 giugno 2009 è stato approvato il Piano operativo per l'attuazione del programma SIRSE che identifica le principali aree di sviluppo per la realizzazione degli obiettivi posti dal programma medesimo, tra cui la realizzazione di un sistema di anonimizzazione dei dati sanitari, servizio infrastrutturale necessario per consentire l'accesso al patrimonio informativo, tramite gli strumenti informatici messi all'uopo a disposizione degli operatori (Data Ware House), nel rispetto delle disposizioni del vigente regolamento regionale (n. 3/R dell'11 maggio 2006) per il trattamento dei dati sensibili sanitari.

Con D.G.R. n. 1-2791 del 25 ottobre 2011, recante ad oggetto "Art. 11 l.r. n. 18/2007. Approvazione proposta di Piano socio-sanitario regionale 2011-2015. Proposta al Consiglio Regionale", si è puntualizzato come l'evoluzione in chiave moderna ed efficiente del SSR non possa prescindere dall'applicazione delle tecnologie dell'informazione (ICT), che oggi consentono agevolmente di supportare con efficacia la gestione delle strutture, di migliorare l'integrazione tra i

diversi nodi dell'assistenza territoriale e dell'assistenza ospedaliera e di facilitare la condivisione dei dati e la comunicazione tra tutti gli attori coinvolti.

Ai sensi degli artt. 20 e 21 del D.L.vo n. 196/2003, la Regione Piemonte ha adottato il regolamento n. 3/R dell'11 maggio 2006 per il trattamento dei dati personali sensibili e giudiziari. Detto regolamento, contenente l'elenco dei trattamenti di competenza della regione, identifica nella scheda n. 12, allegato A, relativa alle attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, le modalità di trattamento dei dati sanitari e di regolazione del relativo flusso informativo.

In relazione alle previsioni della suddetta scheda, la Regione ha manifestato l'esigenza di effettuare l'elaborazione e l'interconnessione, con modalità informatizzate, dei dati personali e sensibili gestiti nell'ambito del Sistema Informativo Sanitario regionale, utilizzando fonti informative prive di elementi identificativi diretti. L'obiettivo istituzionale è quello di valutare e confrontare (tra gruppi di popolazione o tra strutture) a fini programmatori e di controllo, l'appropriatezza, l'efficacia e l'efficienza dell'assistenza erogata, anche con riferimento a specifiche patologie o problematiche sanitarie, avvalendosi di basi dati rese opportunamente anonime, con la possibilità di ricollegare in ogni momento, sulla base delle necessità, gli elementi identificativi.

Con D.G.R. n. 35-352 del 19 luglio 2010 è stato approvato l'avvio del Progetto "Realizzazione del Sistema di Anonimizzazione Reversibile del patrimonio informativo sanitario", per rendere l'accesso al patrimonio informativo sanitario regionale conforme alle previsioni del succitato Regolamento n. 3/R dell'11 maggio 2006, consentendo così alla Regione Piemonte di effettuare gli studi epidemiologici e le analisi sui volumi e sulla tipologia delle prestazioni erogate, necessari per svolgere le proprie attività istituzionali di programmazione e di controllo delle attività sanitarie. Il medesimo atto deliberativo prevedeva altresì che venisse costituito un apposito gruppo di lavoro per sovrintendere alle fasi attuative del progetto di anonimizzazione dei dati sanitari e predisporre, relativamente all'esercizio della funzione di reversibilità dai dati a fronte di qualificate e specifiche esigenze di controllo e verifica, una proposta di identificazione della procedura amministrativa e dei relativi soggetti responsabili.

Con D.D. n. 1071 del 17 dicembre 2010 è stato costituito il succitato Gruppo di Lavoro che, come da previsioni della D.G.R. n. 35–352 del 19 luglio 2010 specificatamente per quanto attiene alla predisposizione, relativamente all'esercizio della funzione di reversibilità dai dati a fronte di qualificate e specifiche esigenze di controllo e verifica, di una proposta di identificazione della procedura amministrativa e dei relativi soggetti responsabili, ha redatto il documento "Anonimizzazione reversibile del patrimonio informativo sanitario regionale: Analisi dei processi ed organizzativa" e, dopo averlo approvato nella riunione del 27 settembre 2011, lo ha trasmesso alla Direzione Sanità.

La Direzione Regionale Sanità, valutati positivamente i contenuti del succitato documento, ha proceduto alla sua rielaborazione, per ricomprendere ed armonizzare nello stesso i processi organizzativi e le relative attività di governo espletate presso l'Assessorato alla Tutela della Salute e Sanità, come risulta nel documento "Disciplinare delle modalità di accesso al patrimonio informativo sanitario regionale e di esercizio della funzione di reversibilità dei dati a fronte di qualificate esigenze", allegato al presente atto deliberativo, parte integrante e sostanziale dello stesso.

Atteso quanto sopra il relatore propone alla Giunta regionale:

- di approvare il documento “Disciplinare delle modalità di accesso al patrimonio informativo sanitario regionale e di esercizio della funzione di reversibilità dei dati a fronte di qualificate esigenze”, allegato al presente atto deliberativo, parte integrante e sostanziale dello stesso, dando atto che esso contiene le indicazioni necessarie per attivare in seno alla Direzione Sanità una apposita funzione di Anonimizzazione, deputata a svolgere le attività regionali previste al fine di:

- ottemperare alle disposizioni del Regolamento Regionale n. 3/R dell’11 maggio 2006
- assicurare il pieno utilizzo del patrimonio informativo regionale per le attività istituzionali di programmazione e di controllo, per gli studi epidemiologici e per le attività di ricerca;

- di incaricare la Direzione Sanità, Settore “Assetto istituzionale ed organizzativo delle ASR e sistemi informativi sanitari”, della gestione della funzione Anonimizzazione, da espletarsi facendo riferimento alle indicazioni contenute nel succitato “Disciplinare delle modalità di accesso al patrimonio informativo sanitario regionale e di esercizio della funzione di reversibilità dei dati a fronte di qualificate esigenze”;

- di dare atto che l’attuazione delle previsioni del presente atto deliberativo non comporta oneri aggiuntivi per la Regione Piemonte;

la Giunta regionale, condividendo le argomentazioni del relatore,

visti:

la legge regionale 15 marzo 1978 n. 13 che ha previsto l’affidamento, per la progettazione degli interventi nel settore informatico, al Consorzio per il Sistema informativo regionale (CSI-Piemonte);

la legge 23 dicembre 1978 n. 833, recante ad oggetto “Istituzione del Servizio Sanitario Nazionale”;

la legge regionale 4 luglio 2005 n. 7, recante ad oggetto “ Nuove disposizioni in procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

la legge regionale 28 luglio 2008 n. 23, recante ad oggetto “Disciplina dell’organizzazione degli uffici regionali e disposizioni concernenti la dirigenza ed il personale”;

il d.lgs 30 giugno 2003 n . 196, recante ad oggetto “Codice in materia di protezione dei dati personali”;

il Regolamento 11 maggio 2006 n. 3/R;

la D.G.R. n. 9-5114 del 22 gennaio 2007, recante ad oggetto “Linee guida del SIRe”;

la D.G.R. n. 15-8626 del 21 aprile 2008, recante ad oggetto “Programma SIRSE-Sistema Integrato Regionale di Sanità Elettronica”;

la D.G.R. n. 10-11162 del 6 aprile 2009, recante ad oggetto “Approvazione del documento “Piano di sviluppo triennale per l’eGoverment e la Società dell’Informazione in Piemonte 2009-2011”;

la D.G.R. n. 1-2791 del 25 ottobre 2011, recante ad oggetto ”Art. 11 l.r. n. 18/2007. Approvazione proposta di Piano socio-sanitario regionale 2011-2015. Proposta al Consiglio Regionale”.

la D.G.R. n. 35–352 del 19 luglio 2010, recante ad oggetto “Approvazione avvio del Progetto "Realizzazione del Sistema di Anonimizzazione Reversibile del patrimonio informativo sanitario" - Disposizioni organizzative.”;

la D.D. n. 1071 del 17 dicembre 2010, recante ad oggetto Costituzione del Gruppo di lavoro a supporto dell’attuazione del Progetto "Realizzazione del Sistema di Anonimizzazione Reversibile del patrimonio informativo sanitario", di cui alla D.G.R. n. 35-352 del 19 luglio 2010;

all’unanimità,

delibera

- di approvare il documento “Disciplinare delle modalità di accesso al patrimonio informativo sanitario regionale e di esercizio della funzione di reversibilità dei dati a fronte di qualificate esigenze”, allegato al presente atto deliberativo, parte integrante e sostanziale dello stesso, dando atto che esso contiene le indicazioni necessarie per attivare in seno alla Direzione Sanità una apposita funzione di Anonimizzazione, deputata a svolgere le attività regionali previste al fine di:

- ottemperare alle disposizioni del Regolamento Regionale n. 3/R dell’11 maggio 2006;

- assicurare il pieno utilizzo del patrimonio informativo regionale per le attività istituzionali di programmazione e di controllo, per gli studi epidemiologici e per le attività di ricerca;

- di incaricare la Direzione Sanità, Settore “Assetto istituzionale ed organizzativo delle ASR e sistemi informativi sanitari”, della gestione della funzione Anonimizzazione, da espletarsi facendo riferimento alle indicazioni contenute nel succitato “Disciplinare delle modalità di accesso al patrimonio informativo sanitario regionale e di esercizio della funzione di reversibilità dei dati a fronte di qualificate esigenze”;

- di dare atto che l’attuazione delle previsioni del presente atto deliberativo non comporta oneri aggiuntivi per la Regione Piemonte;

Avverso la presente deliberazione è ammesso ricorso entro il termine di 60 giorni innanzi al Tribunale amministrativo regionale ovvero ricorso straordinario al Capo dello Stato entro 120 giorni. In entrambi i casi il termine decorre dalla data di piena conoscenza del provvedimento da parte degli interessati.

La presente deliberazione sarà pubblicata sul Bollettino Ufficiale della Regione Piemonte ai sensi dell’art. 61 dello Statuto e dell’art. 5 della L.R. n. 22/2010.

(omissis)

Allegato

Anonimizzazione reversibile del patrimonio informativo sanitario regionale

“Disciplinare delle modalità di accesso al patrimonio informativo sanitario regionale e di esercizio della funzione di reversibilità dei dati a fronte di qualificate esigenze”

1 Introduzione

La normativa relativa al trattamento di dati di interesse sanitario per finalità inerenti "attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria" (art.85, comma 1, lettera C del decreto legislativo 30 giugno 2003 n. 196), ovvero i trattamenti necessari per **"valutare e confrontare l'appropriatezza, l'efficacia e l'efficienza dell'assistenza erogata**" stabilisce che tali attività vengano svolte, da parte dei soggetti autorizzati, su dati privi di elementi identificativi diretti (quindi anonimi).
E' quindi emersa l'esigenza di dotare il Sistema informativo Sanitario Regionale (SISR) di un Sistema di Anonimizzazione Reversibile dei dati, in conformità a quanto prescritto dalla normativa ed in armonia con il modello complessivo di evoluzione del sistema informativo sanitario piemontese.

Alla luce di quanto sopra. La Regione Piemonte ha varato un Progetto di Anonimizzazione del proprio patrimonio informativo sanitario, che prevede la realizzazione di un "**Sistema di Anonimizzazione Reversibile"** dei dati sanitari, per far si che questi vengano archiviati con un codice univoco in luogo dei dati identificativi personali, in modo che la loro consultazione a fini amministrativi non consenta l'identificazione dell'individuo.
Il citato "Sistema di Anonimizzazione Reversibile" prevede che la privazione dei dati personali avvenga all'atto del caricamento dei dati nel DWH regionale, ovvero l'unico ambiente attraverso il quale gli operatori regionali possono accedere al patrimonio informativo sanitario regionale per espletare le attività istituzionali di programmazione e di controllo.
Il Sistema prevede altresì che sia possibile, tramite gli opportuni sistemi di sicurezza nella tenuta degli archivi e strumenti di accesso controllato, ricongiungere i due tipi di informazioni (dati anonimizzato e relativi dati identificativi), solo quando ciò è strettamente necessario ed esclusivamente al personale incaricato.

1.1 Scopo del disciplinare

L'utilizzo del Sistema di Anonimizzazione Reversibile implica la necessità di disporre di regole organizzative che declinino le responsabilità e le modalità operative degli Enti che intervengono nelle operazioni di trattamento del dato, quando questo è soggetto alle limitazioni della scheda 12 dell'allegato A del Regolamento Regionale.

Lo scopo del disciplinare è quello di identificare le regole ed i processi cui tutti i soggetti a vario titolo interessati debbano far riferimento affinché il patrimonio informativo sanitario regionale sia fruibile a supporto delle attività di programmazione e di controllo dei servizi sanitari erogati.

1.1.1 Struttura del disciplinare

Il presente disciplinare è così strutturato:

1. *Obiettivi ed Inquadramento*: una premessa che descrive gli obiettivi dell'analisi condotta, la metodologia utilizzata e l'inquadramento.
2. *Privacy e Sanità*: una descrizione del contesto normativo di riferimento, per evidenziare i concetti fondamentali del Codice Privacy (Dlgs. N. 196/2003) in ambito sanitario e per focalizzare l'attenzione sul DPGR 3/R del 11/05/2006 "Regolamento per il trattamento dei dati personali sensibili e giudiziari".
3. *La rappresentazione sinottica*: una descrizione sintetica dei macroprocessi di riferimento che evidenzia: ruoli, attività, strumenti, tempistiche e finalità.
4. *Assunzioni "organizzative" e di processo*: l'analisi delle "regole di sistema" ossia le regole definite nei singoli macroprocessi in relazione alle fasi di richiesta, autorizzazione, anonimizzazione/reversibilità, erogazione.
5. *Atti organizzativi e strumenti*: la descrizione degli atti organizzativi che Regione Piemonte, come previsto dal DPGR 3/R del 11/05/2006 (Regolamento per il trattamento dei dati personali sensibili e giudiziari"), dovrà adottare per istituire la funzione regionale Anonimizzazione e per individuare la "Struttura Tecnica". Sono descritti i provvedimenti che la funzione regionale Anonimizzazione dovrà adottare per autorizzare le richieste di scarico dati anonimi e di reversibilità
6. *Macroprocess*i: disegno di dettaglio dei processi rilevati

1.2 Riferimenti

I principali documenti ai quali il presente fa riferimento sono i seguenti:

- DGR 35-352 del 19/07/2010 – Approvazione Progetto "realizzazione del sistema di anonimizzazione reversibile del patrimonio informativo sanitario"
- Determina dirigenziale n.499 del 28 Luglio 2010 Prot. 23438/DB2003
- Proposta Tecnico Economica "*ADS—PTE-01-V09-Anonimizzazione.doc Paragrafo 8.1.1*"
- Il Dlgs. N. 196/2003: art. 4 – artt. 28-29-30
- Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli Enti e Agenzie regionali, degli Enti vigilati dalla Regione (articoli 20 e 21 del decreto legislativo 30 giugno 2003 n. 196 (codice in materia di protezione dei dati personali) emanato con Decreto del Presidente della Giunta Regionale 11 maggio 2006, n. 3/R; in particolare Scheda 12 Allegato A
- DD 1071 del 17/12/2010 (Costituzione del GdL Anonimizzazione)
- Documento "Analisi di processi ed organizzativa" nella sua versione definitiva "*ADS-06-PRE-01-V14 Analisi processi*", approvato dal GDL Regionale il 28 giugno 2011.

1.3 Glossario

- **GDL Regionale:** è il Gruppo di Lavoro istituito da Regione Piemonte ai sensi della DGR 35-352 del 19/07/2010 con DD 1071 del 17/12/2010 per sovrintendere alle fasi attuative del progetto e predisporre, relativamente all'esercizio della funzione di reversibilità dai dati a fronte di qualificate e specifiche esigenze di controllo e verifica, una proposta di identificazione della procedura amministrativa e dei relativi soggetti responsabili.
- **S.R. Anonimizzazione** : struttura regionale presso cui è stata resa operativa la funzione di anonimizzazione.
- **ADS**: acronimo per il progetto Anonimizzazione Dati Sanitari (reversibili).
- **Patrimonio Informativo Sanitario Regionale:** è il patrimonio informativo di interesse sanitario di cui Regione Piemonte è titolare, rappresenta l'insieme dei flussi informativi regionali acquisiti dalle ASR Regionali. La raccolta dei dati dei flussi informativi in ambito Sanità Regione ed in particolare quelli relativi alla mobilità regionale, risalgono al 1998 sulla base della delibera di Giunta Regionale nr. 31-26419 del 30/12/1998 che recepiva le necessità di una raccolta sistematica per consentire lo scambio di informazioni tra regioni e il monitoraggio regionale.
- **DWHPADDI** (Piattaforma Analisi Dati Decisionali Integrati). PADDI è in particolare il punto di accesso, unico ed organizzato, ai dati presenti sul datawarehouse o **DWH** della sanità regionale. PADDI è un progetto incrementale che prevede la messa a disposizione di report e strumenti di interrogazione ed analisi dei dati presenti nel DWH in formato "aggregato" sulle seguenti tematiche:

    - Prestazioni sanitarie;
    - Schede di dimissione ospedaliere;
    - Prescrizioni farmaceutiche;
    - Certificati di assistenza al parto (CEDAP);
    - Mobilità regionale;
    - Mobilità nazionale;
    - Registro Diabetici.

- **SDS:** è l'acronimo di Sportello Dati Sanitari e viene indicato come l'eventuale strumento tecnico di front-end per gestire le richieste e le relative consegne di scarico "massivo" di dati anonimi. Al momento della redazione di questo disciplinare l'utilizzo dell'attuale sistema SDS è in fase di valutazione.
- **SR:** è l'acronimo di Servizio di Reversibilità. Viene indicato come lo strumento tecnico di front-end che gestisce le richieste e le relative consegne di reversibilità di dati anonimi.
- **Ente citato in Scheda 12:** sono gli Enti citati nella Scheda 12 Allegato A del DPGR 3/R del 11/05/2006 "Regolamento per il trattamento dei dati personali sensibili e giudiziari": *Regione Piemonte, ARESS, Istituti Scientifici Regionali in ambito sanitario (es. Rete di Epidemiologia), ARPA*
- **Ente non citato in Scheda 12:** sono gli Enti Regionali e non Regionali che non sono espressamente citati citati nella Scheda 12 Allegato A del DPGR 3/R del 11/05/2006 "Regolamento per il trattamento dei dati personali sensibili e giudiziari".

- **Ente Regionale:** comprende Regione Piemonte e suoi Enti strumentali/ausiliari.
- **Ente non Regionale:** sono Enti Nazionali quali il Ministero della Salute ed altri Enti giuridicamente non regionali quali UniTo, PoliTo.
- **Dato anonimo:** è il dato che, in origine o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile ai sensi del Codice Privacy (Decreto 196/2003). Non c'è possibilità di identificazione nelle statistiche: il conoscere le abitudini di un gruppo di persone attraverso percentuali, non ci permette di risalire all'identità dei singoli soggetti. Non sono anonimi i dati sanitari che identificano i pazienti solo con un codice, o campi relativi alle prime lettere del cognome e nome associati a indicazioni di data di nascita e sesso.
- **Dato in chiaro:** è il dato personale che permette l'identificazione del soggetto.
- **Dato "reversato":** è il dato anonimo che, sottoposto alla funzione di reversibilità, viene trasformato in dato in chiaro per consentire l'identificazione del soggetto.
- **Bruciatura ID Anonimo:** è la situazione nella quale, attraverso elaborazioni statistiche, è possibile risalire all'associazione dell'ID Anonimo "muto" con gli identificativi diretti della persona. Il meccanismo con cui una re-identificazione può avvenire può essere immediato (avendo a disposizione contemporaneamente il codice anonimo ed il corrispondente dato anagrafico) o affidato ad algoritmi di abbinamento di informazioni (record linkage, statistical matching, ecc.).
- **Identificativo Diretto:** è il dato personale che consente l'identificazione diretta del soggetto interessato, quale il nome, il cognome, il codice fiscale
- **Identificativi Indiretti**: l'insieme dei dati di per sé anonimi, che consentono l'indiretta identificazione del soggetto. L'insieme dei mezzi che possono ragionevolmente essere impiegati per identificare l'interessato, in un database privo di identificativi diretti. Possono essere dati in possesso anche di terzi.
  L'identificazione di un soggetto si verifica ad esempio quando si riesce a stabilire una relazione biunivoca tra la combinazione delle modalità dei dati identificativi indiretti di un'unità presente nel file di dati rilasciati e l'unità dell' archivio nominativo in possesso di terzi. Dato il rischio di identificazione indiretta dei soggetti, i dati sanitari individuali, come previsto dall'art 22 Codice Privacy) non possono essere "diffusi", ossia portati a conoscenza di chiunque, in qualunque forma compresa la loro messa a disposizione o consultazione on line (possono essere invece pubblicati, ossia diffusi, i soli dati statistici).La comunicazione dei dati sanitari individuali ai soggetti autorizzati, anche mediante accessi on line al sistema, sarà invece soggetta a identificazione e tracciatura.
- **Provvedimento Autorizzativo:** è il provvedimento che dovrà essere adottato per autorizzare il trattamento dei dati anonimi o "reversati" agli Enti richiedenti**.**

2 Obiettivi ed Inquadramento

Il trattamento dati di competenza della Regione, regolamentato nella *scheda 12 dell'allegato A del DPGR 3/R del 11/05/2006,* ha l'obiettivo di valutare l'appropriatezza, l'efficacia, l'efficienza dell'assistenza sanitaria erogata. Da ciò ne consegue l'esigenza di poter ricostruire i percorsi assistenziali e di elaborare ed interconnettere le diverse banche dati costituenti il Patrimonio Informativo Regionale di interesse sanitario, per i quali esiste una specifica componente sul DWH sanitario regionale.
Nel rispetto dei principi di necessità e di non eccedenza rispetto alle finalità perseguite, il suddetto trattamento deve avvenire con dati privati degli elementi identificativi diretti, tramite l'assegnazione di un codice univoco (c.d. "anonimo"), che non consenta l'identificazione dell'interessato durante il trattamento del dato.

La realizzazione del sistema di anonimizzazione implica necessariamente alcune modifiche nell'operatività dell'organizzazione regionale e l'obiettivo del presente disciplinare è proprio quello di identificare le regole di processo cui l'organizzazione regionale debba far riferimento per gestire il Sistema di Anonimizzazione Reversibile dei Dati Sanitari, nel rispetto delle previsioni della **scheda 12 dell'allegato A** del Regolamento Regionale ed in particolare:

- le regole e i processi che dovranno essere osservati dalla "struttura tecnica" per la gestione del sistema di anonimizzazione;
- il processo che descrive le modalità attraverso cui la "S.R. Anonimizzazione" invierà le richieste di reversibilità dei dati alla "struttura tecnica";
- il processo che descrive le modalità attraverso le quali la "struttura tecnica" gestirà le richieste di anonimizzazione dei flussi provenienti da enti esterni.

3 Il Contesto normativo di riferimento: Privacy e Sanità

Per quanto riguarda la normativa in materia di protezione dei dati personali, il trattamento dati in relazione alle diverse attività del servizio sanitario avviene sulla base di:

- Disposizioni generali e specifiche del Dlgs. 96/03;
- Specifiche leggi e regolamenti che disciplinano adeguatamente alcuni trattamenti dati, individuando anche i dati che devono essere trattati e le operazioni da effettuare;
- Regolamento n. 3/R del 11/05/2006, per il trattamento dei dati sensibili e giudiziari da parte della Regione Piemonte,aziende sanitarie,enti, aziende ed agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo.

3.1 Alcune Definizioni

Dal codice Privacy (Dlgs. 196/2003) sono riportate alcune definizioni dall'art. 4.

- **Dato Personale** qualunque informazione relativa a persona fisica o giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
- **Dati Identificativi:** i dati personali che permettono l'identificazione diretta dell'interessato.
- **Dati Anonimi***:* il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
- **Dati Sensibili:** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, politico, filosofico o sindacale, nonché **i dati personali idonei a rivelare lo stato di salute e la vita sessuale**.
- **Dati Giudiziari:** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale

3.2 Soggetti che effettuano il trattamento

Dal codice Privacy (Dlgs. 196/2003) sono riportate le definizione dei soggetti che effettuano il trattamento con una sintesi dei loro ruoli e compiti.

- **Art. 28. Titolare del trattamento:** Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.Il Codice ha formalmente introdotto la figura del contitolare (espressamente prevista anche nel modello di notificazione predisposto dal Garante).

  Ruoli e Compiti
  - Definisce una corretta impostazione delle modalità da seguire per il trattamento dei dati e delle correlative misure di sicurezza.
  - Può nominare (facoltativamente) uno o più Responsabili del trattamento dati.

- **RESPONSABILE: art. 4 lettera h** E' la persona fisica o giuridica direttamente preposta dal Titolare con funzioni di organizzazione e controllo dei trattamenti. Il *Responsabile* effettua il trattamento attenendosi alle istruzioni impartite dal *Titolare* il quale vigila sulla puntuale osservanza delle disposizioni. La nomina del Responsabile è facoltativa.

  Ruoli e Compiti
  - Non può nominare un altro responsabile.
  - Nomina gli Incaricati al trattamento dei dati affidati.
  - Sorveglia che il trattamento sia effettuato nei termini e nei modi stabiliti nel TU Privacy.
  - Impartisce istruzioni agli incaricati al trattamento.
  - Periodicamente verifica le condizioni per conservare ed aggiornare i profili di autorizzazione degli incaricati.
  - Redige annualmente il doc. programmatico sulla Sicurezza.

- **INCARICATO:** Dall'art. 30: "Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Ruoli e Compiti

- Effettua le operazioni di trattamento dati sulla base di quanto regolamentato per iscritto dal Titolare/Responsabile. Le sue responsabilità possono variare in funzione del grado di dettaglio dei compiti impartiti.

- **INTERESSATO: art. 4 lettera i** L'Interessato è la persona fisica, la persona giuridica, l'Ente o l'Associazione cui si riferiscono i dati personali.

Ruoli e Compiti

- In base all'art.7 D.Lgs. 196/2003 ha il diritto di richiedere dell'esistenza o meno dei suoi dati; di avere comunicazione, di conoscere l'origine, la finalità,la modalità del trattamento; la logica applicata; gli estremi identificativi del titolare, del responsabile e dell'incaricato.
- Ha anche il diritto di ottenere l'aggiornamento, la rettifica e l'integrazione; la cancellazione, la trasformazione ed il blocco dei dati nonché di opporsi al trattamento di dati anche se pertinenti allo scopo.

3.3 Regolamento Regionale Trattamento Dati Sensibili e Giudiziari

In data 11 maggio 2006, con decreto del Presidente della Giunta Regionale in attuazione della deliberazione del Consiglio Regionale n.65-15263 del 9 maggio 2006, Regione Piemonte ha adottato il "**Regolamento regionale per il trattamento dei dati personali sensibili e giudiziari**".
Il **Regolamento riguarda** Il trattamento dati sensibili e giudiziari per finalità di rilevante interesse pubblico effettuati da Regioni, Aziende Sanitari, Enti/Servizi ed agenzie regionali,.

Il Regolamento è articolato in tre allegati, ciascuno dei quali a sua volta composto da schede che riguardano i singoli trattamenti. In particolare, gli allegati A e B si distinguono per le diverse finalità dei trattamenti.

- **Allegato A Trattamenti delle Regioni e degli Enti Regionali** contiene l'elenco dei trattamenti di competenza delle Regioni, degli Enti, delle Agenzie regionali e degli enti controllati e vigilati dalle Regioni:

1. Attività amministrative correlate agli interventi di prevenzione, diagnosi, cura e riabilitazione (gestione della mobilità sanitaria, ...);
2. Attività di certificazione e vigilanza sulle sperimentazioni;
3. Gestione dei rapporti con i soggetti accreditati e convenzionati;
4. Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria (***Scheda 12: trattamento dati privi degli elementi identificativi diretti "anonimi").***

Per tali fini la Regione deve effettuare, sulla base di **dati anonimi,** l'elaborazione e l'interconnessione dei dati personali gestiti nell'ambito dei diversi archivi del Patrimonio Informativo Sanitario Regionale.
Nello specifico la **scheda 12**, dell'allegato A, (relativo ai trattamenti di competenza della Regione), riguarda il trattamento di dati per finalità inerenti "*attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria*" (art.85, comma 1, lettera b) ovvero comprende quei trattamenti necessari per *"monitoraggio e valutazione dell'efficacia dei trattamenti sanitari erogati, di valutazione dell'appropriatezza e della qualità dell'assistenza, di valutazione della soddisfazione dell'utente e di valutazione dei fattori di rischio per la salute"*.
Per tali scopi le funzioni regionali negli ambiti indicati a Regione devono trattare i dati privati di elementi identificativi diretti (anonimi).
La scheda 12 dell'allegato A descrive pertanto i requisiti che il Sistema di Anonimizzazione Reversibile dei dati deve rispettare e la cui realizzazione è stata commissionata da Regione Piemonte al CSI – Piemonte.

- **Allegato B Trattamenti delle Aziende Sanitarie** per finalità dei trattamenti:

1. Attività amministrative correlate agli interventi di prevenzione, diagnosi, cura e riabilitazione, in relazione ai diversi tipi di servizi erogati;
2. Attività di certificazione (compresa l'attività medico legale);
3. Applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;
4. Attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria (***Scheda 39: trattamenti di dati comprensivi degli identificativi diretti***).

4 La rappresentazione sinottica

I macroprocessi di riferimento sono quattro:
1) Scarico Anonimo Standard
2) Scarico Anonimo Temporaneo
3) Scarico Anonimo con anonimizzazione fonte dati esterna
4) Reversibilità scarico anonimo standard.

La visone "sinottica" dei processi di riferimento ha l'obiettivo di identificare **chi** fa che **cosa**, **come**, **quando** e **perché** viene fatta quella cosa e con quale impatto sugli altri componenti dell'organizzazione.

4.1 I Ruoli

Sono di seguito descritti **i ruoli** dei processi organizzativi di anonimizzazione dei dati sanitari.
Per ciascun ruolo individuato, vengono indicati a quali soggetti indicati dalla legge Privacy è applicabile nonché quali sono i principali attori coinvolti.

RICHIEDENTE DATO ANONIMO
Esprime la necessità di effettuare un'attività di programmazione, gestione e valutazione dell'assistenza sanitaria con relativa elaborazione di dati anonimi.
Il richiedente dati anonimi diventa fruitore degli stessi previa formale autorizzazione di Regione Piemonte.

Può essere una figura diversa da quelle indicate alla Scheda 12 Allegato A del Regolamento Regionale.

Esempi di attori principali sono:

- **Ente citato in Scheda 12:** Regione Piemonte, ARESS, Istituti Scientifici Regionali in ambito sanitario (es. Rete di Epidemiologia Piemonte), ARPA.
- **Ente non citato in Scheda 12**: UniTo, PoliTo, CoTo, Ministero della Salute, Enti strumentali/ausiliari di Regione Piemonte, altre.

RICHIEDENTE DATO IN CHIARO
Esprime la necessità di effettuate un'attività (per finalità di assistenza, cura o giudiziaria) utilizzando gli identificativi in chiaro ("dati reversati") individuati in seguito ad una attività con dati anonimi.

E' il soggetto, persona fisica e giuridica, nominato (Dlgs, 196/2003) Titolare/Responsabile del trattamento per finalità diversa dalla Scheda 12 (esempio erogare un servizio).

Esempi di attori principali sono:
- Regione Piemonte,
- ASR,
- Autorità giudiziaria
- Ministero competente

FRUITORE DATO IN CHIARO
E' il soggetto autorizzato (destinatario) al quale devono essere comunicati i dati in chiaro "reversati", in seguito all'esito dell'attività condotta.
E' il soggetto, persona fisica e giuridica, nominato (Dlgs. 196/2003) **Responsabile/Incaricato del trattamento per finalità diversa dalla Scheda 12** (esempio erogare un servizio assistenza sanitaria).

Esempi di attori principali sono:
- Regione Piemonte,
- ASR,
- Autorità giudiziaria,
- Ministero competente

AUTORIZZATORE
La struttura regionale appositamente incaricata.

FORNITORE ESTERNO (dati sanitari e non)

Ha la titolarità dei dati esterni che possono eventualmente essere richiesti nella conduzione dell'attività programmatica di valutazione sanitaria

E' il soggetto titolare di banche dati esterne ed in quanto tale autorizza l'utilizzo di tali banche dati.

Esempi di attori principali sono:

- Enti regionali (archivio in possesso di un ente regionale non presente nel DWH),
- Ente non regionale (esempi INPS, INAIL, etc…)

STRUTTURA TECNICA

E' la funzione tecnica che elabora i dati in chiaro di Regione Piemonte per attribuirne l'id anonimo e gestirne la reversibilità.

E' il soggetto, nominato tramite apposito atto (ai sensi del Dlgs. 196/2003) dal Titolare, Responsabile Esterno del trattamento dati in chiaro.

CSI-Piemonte è ad oggi il soggetto che svolge le funzioni di Struttura Tecnica, in quanto nominato Responsabile Esterno del trattamento dati da parte di Regione Piemonte, come previsto dal DPGR 3/R del 11/05/2006 (Regolamento per il trattamento dei dati personali sensibili e giudiziari).

4.2 Autorizzazione permanente per lo scarico dati anonimi

Chi?	L'AUTORIZZATORE ossia la S.R. Anonimizzazione e la STRUTTURA TECNICA
Cosa?	L'AUTORIZZATORE autorizza gli enti/servizi citati in scheda 12 a fruire dei dati sanitari anonimi.
	La STRUTTURA TECNICA riceve le informazioni relative all'autorizzazione permanente concessa dalla S.R. Anonimizzazione.
Come?	L'AUTORIZZATORE predispone il provvedimento autorizzativo permanente e lo comunica sia agli Enti citati in Scheda 12 sia alla STRUTTURA TECNICA che registra sul sistema SDS l'autorizzazione permanente concessa.
Quando?	L'autorizzazione permanente a fruire dei dati anonimi per gli Enti citati in scheda 12 viene effettuata all'avvio del sistema di Anonimizzazione Reversibile dei dati sanitari.
Perché?	La STRUTTURA TECNICA deve essere in grado di identificare nel sistema gli Enti richiedenti che possiedono l'autorizzazione regionale permanente (Enti citati in scheda 12).

4.3 Scarico dati anonimi ID Standard

Chi?	Il RICHIEDENTE DATO ANONIMO che deve essere un Ente con autorizzazione permanente e la STRUTTURA TECNICA che gestisce il sistema d'anonimizzazione reversibile dei dati sanitari.
Cosa?	Il RICHIEDENTE DATO ANONIMO richiede lo scarico di dati sanitari anonimi disponibili nel DWH regionale. La STRUTTURA TECNICA prende in carico la singola richiesta di scarico dati con ID anonimo standard, la elabora, consegna i dati, li archivia e li traccia.
Come?	Il RICHIEDENTE DATO ANONIMO effettua apposita richiesta di scarico dati standard (completa di allegato tecnico), attraverso l'accesso sicuro allo strumento SDS. La STRUTTURA TECNICA, sempre attraverso lo strumento SDS, traccia, elabora ed evade le singole richieste pervenute.
Quando?	Il RICHIEDENTE DATO ANONIMO per ogni singola richiesta di scarico di dati sanitari di dettaglio anonimi. La STRUTTURA TECNICA ogni volta che sullo strumento di sportello dati (SDS) viene registrata una richiesta di scarico da parte di un richiedente autorizzato.
Perché?	Il RICHIEDENTE DATO ANONIMO per il trattamento dei dati sanitari anonimi con finalità scheda 12. La STRUTTURA TECNICA, quale "Responsabile Esterno al Trattamento dei dati" che svolge la funzione tecnica di elaborare le richieste di scarico dati anonimi del DWH sanitario regionale.

4.4 Scarico dati anonimi ID Temporanei

Chi?	Il RICHIEDENTE DATO ANONIMO che deve essere un **Ente non citato in Scheda 12.** L'AUTORIZZATORE che valuta ed eventualmente autorizza le singole richieste. La STRUTTURA TECNICA che gestisce il sistema d'anonimizzazione reversibile dei dati sanitari.
Cosa?	Il RICHIEDENTE DATO ANONIMO effettua richiesta di scarico di dati sanitari anonimi disponibili nel DWH, chiedendo alla S.R. Anonimizzazione la relativa autorizzazione. L'AUTORIZZATORE valuta la richiesta ed in caso positivo fornisce un'autorizzazione temporanea. La STRUTTURA TECNICA riceve dalla S.R. Anonimizzazione l'autorizzazione temporanea concessa al richiedente, prende in carico la specifica richiesta di scarico di dati con ID temporaneo, la elabora, consegna i dati, li archivia e li traccia.
Come?	Il RICHIEDENTE DATO ANONIMO contatta la S.R. Anonimizzazione, compila la relativa modulistica di richiesta/autorizzazione allo scarico dei dati anonimi con ID temporaneo. L'AUTORIZZATORE: • predispone il provvedimento autorizzativo temporaneo, lo protocolla e lo inoltra al RICHIEDENTE DATO ANONIMO ed alla STRUTTURA TECNICA; • accede ad SDS per registrare l'autorizzazione temporanea e la richiesta di scarico per conto del richiedente. La STRUTTURA TECNICA attraverso SDS: • riceve l'informazione relativa all'autorizzazione temporanea concessa all'Ente richiedente e per specifica richiesta; • procede alla tracciatura, elaborazione, evasione della singola richiesta autorizzata.
Quando?	Il RICHIEDENTE DATO ANONIMO per ogni singola richiesta di scarico di dati sanitari anonimi di dettaglio. L'AUTORIZZATORE ogni volta che viene contattato per un richiesta di scarico dati sanitari anonimi da parte di Enti non citati in Scheda 12. La STRUTTURA TECNICA ogni volta che sullo strumento di sportello dati (SDS) viene registrata una richiesta di scarico da parte della S.R. Anonimizzazione (AUTORIZZATORE) per conto del RICHIEDENTE DATI ANONIMI.
Perché?	Il RICHIEDENTE DATO ANONIMI è un Ente non citato in scheda 12 che deve effettuare un trattamento di dati sanitari anonimi. La STRUTTURA TECNICA, quale "Responsabile Esterno al Trattamento dei dati" che svolge la funzione tecnica di elaborare le richieste di scarico dati anonimi del DWH Regionale Sanitario per attribuirne l'ID anonimo temporaneo.

4.5 Scarico dati anonimi con anonimizzazione di dati esterni

Chi?	Il RICHIEDENTE DATO ANONIMO che di norma è un **Ente citato in Scheda 12.** Nel caso in cui fosse un Ente non citato in scheda 12, si rimanda alle schede di regolamento qualora previste ed alle norme di legge. L'AUTORIZZATORE che valuta ed eventualmente autorizza le singole richieste (In presenza di fonte esterna da anonimizzare si parla sempre di *Autorizzazione Temporanea,* benché in presenza di un richiedente citato in scheda 12).

	Il FORNITORE ESTERNO che detiene la titolarità della fonte di dati sanitari o non sanitari per la quale è richiesta l'anonimizzazione. La STRUTTURA TECNICA che gestisce il sistema d'anonimizzazione reversibile dei dati sanitari.
Cosa?	Il RICHIEDENTE DATO ANONIMO: • richiede autorizzazione allo scarico "dati anonimi" con fonte esterna; • contatta il Titolare della fonte esterna (in caso la fonte esterna sia fornita da un ente terzo) per richiedere la nomina della STRUTTURA TECNICA a Responsabile Esterno al trattamento dati della fonte esterna medesima. L'AUTORIZZATORE valuta la richiesta ed in caso positivo fornisce l'autorizzazione temporanea (ad hoc). Il FORNITORE ESTERNO: • nomina la STRUTTURA TECNICA quale Responsabile Esterno al trattamento dei propri dati in chiaro (limitatamente al contenuto della specifica fonte esterna); • invia l'archivio dati in chiaro alla STRUTTURA TECNICA per consentire a questa di evadere la richiesta di anonimizzazione. La STRUTTURA TECNICA: • riceve dal FORNITORE ESTERNO (Titolare) l'atto di nomina a Responsabile Esterno al Trattamento dati in chiaro della fonte esterna; • acquisisce la fonte dati esterna utilizzando strumenti in modalità sicura; • prende in carico la richiesta di scarico dati anonimi con anonimizzazione di fonte esterna, elabora, consegna i dati, li archivia e li traccia.
Come?	Il RICHIEDENTE DATO ANONIMO contatta la S.R. Anonimizzazione, compila la relativa modulistica di richiesta scarico dati anonimi con anonimizzazione di dati esterni. L'AUTORIZZATORE: • predispone il provvedimento regionale autorizzativo temporaneo, lo inoltra al RICHIEDENTE DATO ANONIMO ed alla STRUTTURA TECNICA; • accede ad SDS per registrare l'autorizzazione temporanea e la richiesta di scarico per conto del richiedente. La STRUTTURA TECNICA attraverso l'utilizzo di strumenti di interscambio dati "sicuri": • riceve ed archivia l'informazione relativa all'autorizzazione temporanea concessa all'Ente richiedente e per specifica richiesta; • procede alla tracciatura, elaborazione, evasione della singola richiesta autorizzata; • prende in carico, acquisisce, archivia, traccia la fonte dati esterna da anonimizzare,
Quando?	Il RICHIEDENTE DATO ANONIMO per ogni singola e specifica richiesta di scarico di dati sanitari di dettaglio anonimi con anonimizzazione di dati esterni. L'AUTORIZZATORE ogni volta che viene contattato per un richiesta di scarico dati sanitari con fonte esterna da anonimizzare. La STRUTTURA TECNICA ogni volta che sullo strumento di sportello dati (SDS) viene registrata una richiesta di scarico con anonimizzazione di dati esterni da parte della S.R. Anonimizzazione (AUTORIZZATORE).
Perché?	Il RICHIEDENTE DATO ANONIMO per svolgere le proprie attività di competenza ha la necessità di correlare ("linkare") dati sanitari anonimi con altri dati non appartenenti al patrimonio informativo sanitario regionale o non presenti nel DWH Sanitario. L'AUTORIZZATORE valuta eventuali rischi di bruciatura del codice anonimo. La STRUTTURA TECNICA, quale Responsabile Esterno al Trattamento dei dati che svolge la funzione tecnica di elaborare le richieste di scarico dati anonimi del DWH Regionale Sanitario per attribuirne l'ID anonimo temporaneo.

4.6 Reversibilità dati anonimi

Chi?	Il RICHIEDENTE DATO ANONIMO; il RICHIEDENTE DATO IN CHIARO; il FRUITORE DATO IN CHIARO; l'AUTORIZZATORE; la STRUTTURA TECNICA.
Cosa?	Il RICHIEDENTE DATO ANONIMO rileva la necessità di reversibilità dei dati sanitari anonimi trattati ed individua il richiedente/fruitore del dato in chiaro. Il RICHIEDENTE DATO IN CHIARO richiede autorizzazione alla reversibilità di un set di ID anonimi (standard). Il FRUITORE DATO IN CHIARO utilizza i dati in chiaro "reversati" per fini diversi dalla scheda 12. L'AUTORIZZATORE effettua le proprie valutazioni, avvalendosi del supporto tecnico del Gruppo di Lavoro Anonimizzazione, che viene di volta in volta chiamato a formalizzare uno specifico parere, ed in caso questo sia positivo, fornisce un'autorizzazione ad hoc. **In caso di richiesta da parte dell'Autorità Giudiziaria l'autorizzazione non è necessaria**. La STRUTTURA TECNICA prende in carico la richiesta di reversibilità, la registra e consegna i dati archiviandoli e tracciandoli.
Come?	Il RICHIEDENTE DATO ANONIMO invia al RICHIEDENTE DATO IN CHIARO le specifiche tecniche del trattamento dati effettuato o l'elenco degli ID anonimi da "reversare". Il RICHIEDENTE DATO IN CHIARO contatta la S.R. Anonimizzazione, compila la modulistica per chiedere la reversibilità (completa delle specifiche tecniche). Il FRUITORE DATO IN CHIARO concorda con la STRUTTURA TECNICA le modalità "sicure" di consegna. L'AUTORIZZATORE predispone la nota di accettazione/diniego della richiesta, la trasmette al RICHIEDENTE ed al FRUITORE DEL DATO IN CHIARO e, in caso di autorizzazione, anche alla STRUTTURA TECNICA. La STRUTTURA TECNICA traccia la richiesta, elabora e consegna i dati in chiaro tramite il servizio SR.
Quando?	Il RICHIEDENTE DATO IN CHIARO ogni volta che riceve specifica richiesta da un FRUITORE DATO ANONIMO. Il FRUITORE DATO IN CHIARO che riceve una segnalazione da un FRUITORE DATO ANONIMO. L'AUTORIZZATORE ogni volta che viene contattato per una richiesta di reversibilità. La STRUTTURA TECNICA ogni volta che l'AUTORIZZATORE trasmette la modulistica recante la richiesta di reversibilità e la relativa nota autorizzativa.
Perché?	Il RICHIEDENTE/FRUITORE DATO ANONIMO, a seguito del trattamento di dati sanitari anonimi, avverte la necessità di disporre di dati identificativi "in chiaro" per esigenze diverse da quelle della scheda 12. Il RICHIEDENTE/FRUITORE DATO IN CHIARO, che ha finalità diverse da quelle di programmazione e di controllo di cui alla scheda 12, può richiedere dati sanitari in chiaro, nel rispetto della regola del POS, per evitare bruciature del codice anonimo. L'AUTORIZZATORE: la Scheda 12 prevede che la regione debba definire modalità e procedure per l'utilizzo della funzione di reversibilità. La STRUTTURA TECNICA quale "Responsabile Esterno al trattamento dati" che svolge la funzione tecnica di "reversare" i dati anonimi presenti sul DWH sanitario regionale.

4.7 Attori e Finalità

Le finalità per le richieste di scarico dati sanitari anonimi sono sempre quelle previste nella Scheda 12 dell'allegato A del Regolamento n. 3/R del 11/05/2006, per il trattamento dei dati personali, sensibili e giudiziari da parte della Regione Piemonte, delle aziende sanitarie, degli enti, delle aziende ed agenzie regionali e dei soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo.
Lo schema che segue rappresenta la sintesi delle regole condivise rispetto ai diversi attori coinvolti nei processi analizzati.

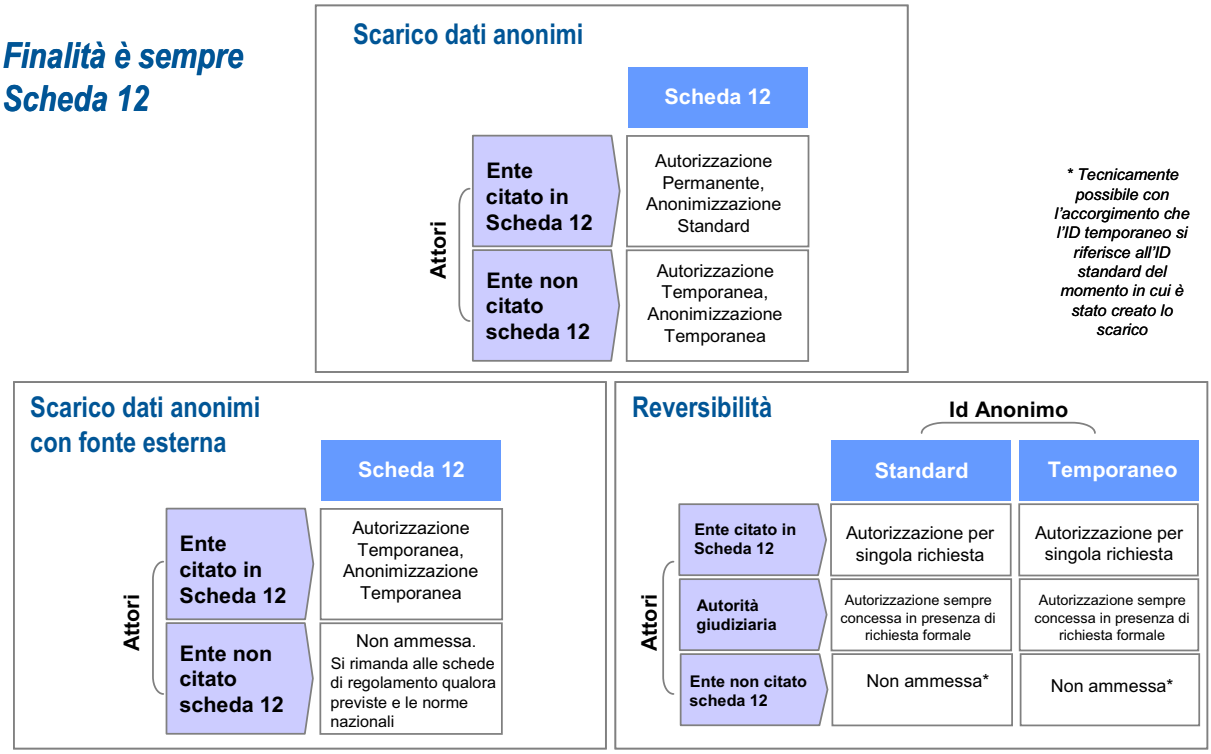

Figura 1 - Attori e Finalità - schema di sintesi

5 Il Sistema d'Anonimizzazione Reversibile Dati Sanitari

Il sistema di anonimizzazione reversibile dei dati sanitari deve consentire attraverso il DWH Regionale Sanitario, la gestione del dato in forma anonima per quanto attiene ai:

- dati inviati dalle ASR/Enti Privati attraverso il flussi;
- dati contenuti nelle basi dati degli applicativi utilizzati dalle ASR, che fanno parte del SISR, e per i quali esiste una componente di DWH.

5.1 La Mappatura degli Archivi dei Dati Sanitari oggetti di anonimizzazione

I principali archivi dati citati nella a Scheda 12 – Allegato A del Regolamento Regionale per il trattamento dei dati personali sensibili e giudiziari (Art. 20-21 D.Lgs 196/2003 Codice in materia di dati personali), come risultato alla data della redazione di questo disciplinare, sono sotto riportati nella tabella "***Mappatura Archivi Sanitari***", dove vengono presentati in correllazione rispetto:

- ai Flussi Informativi Regionali attualmente gestiti;
- ai dati provenienti dagli applicativi operazionali delle singole ASR, facenti parte del patrimonio informativo sanitario regionale.

Questi archivi costituiscono la principale fonte di informazioni a fini epidemiologici o di ricerca e per tal scopo dovranno essere privati degli elementi identificativi diretti subito dopo la loro acquisizione da parte della Regione stessa.
Nella tabella che segue sono indicati gli archivi oggetto di anonimizzazione citati in Scheda 12, i corrispondenti Flussi Regionali (Patrimonio Informativo Sanitario Regionale) e le componenti del DWH Sanitario (PADDI) che alla data del presente disciplinare si trovano negli stati indicati:

- **esistente**;
- **pianificata** attività evolutiva verso DWH PADDI nell'anno 2011;
- **da valutare** attività evolutiva DWH PADDI;
- **prevista** attività evolutiva verso DWH PADDI **ma non pianificata** nell'anno 2011;
- **in corso di realizzazione** attività evolutiva verso DWH PADDI entro l'anno 2011;
- **non prevista** evolutiva verso DWH PADDI;
- **sospesa / da ripianificare** attività evolutiva verso DWH PADDI:
- n.a.: non applicabile (non esiste il flusso regionale di riferimento).

Tabella 1- Mappatura Archivi Sanitari (Archivi Sk 12 / Flussi Regionali/ DWH PADDI) – Aggiornato a Luglio 2011.

Archivi Dati da Scheda 12	Flusso di riferimento	DB Operazionale di riferimento	Componente DWH PADDI	Stato	Note
Assistenza specialistica ambulatoriale e riabilitativa	C (Specialistica Ambulatoriale)		DWH Prestazioni	Esistente	
	C2 (Pronto Soccorso)		DWH Prestazioni	Esistente	
	C4 - Specialistica Ambulatoriale: - prestazioni erogate all'assistito durante il ricovero ospedaliero presso l'azienda sanitaria		DWH Prestazioni	Esistente	
	C5 - Specialistica Ambulatoriale: - prestazioni a fatturazione e pagamento diretto tra aziende		DWH Prestazioni	Esistente	
Emergenza sanitaria e 118	C2 (Pronto Soccorso/Prestazioni DEA)		DWH Prestazioni	Esistente	
	EMUR (Emergenza/Urgenza)		DWH 118 – Emergenza Sanitaria	Pianificato per anno 2011	
	G (Trasporto con ambulanza ed elisoccorso)			Previsto ma non pianificato per il 2011	
Assistenza residenziale e semiresidenziale	FAR (Prestazioni residenziali e semi residenziali)		DWH FAR-SIAD	Esistente	
Assistenza domiciliare	SIAD (Assistenza Domiciliare)		DWH FAR-SIAD	Esistente	
Assistenza ospedaliera	SDO (o Flusso A)		DWH SDO (Schede Dimissione Ospedaliere)	Esistente	
Assistenza farmaceutica e farmacovigilanza	Farmaceutica Convenzionata (Somministrazione Farmaci attraverso ricetta medica del medico di medicina generale)		DWH Farmaceutica	Esistente	
	F (Somministrazione Diretta Farmaci) somministrazione e/o erogazione diretta di farmaci da parte delle strutture ospadaliere a cittadini non ricoverati		DWH Farmaceutica	Esistente	La parte di file F è in corso di realizzazione
	D (Farmaceutica dei non residenti)		DWH Farmaceutica	Esistente	

Archivi Dati da Scheda 12	Flusso di riferimento	DB Operazionale di riferimento	Componente DWH PADDI	Stato	Note
Assistenza termale	**E (Cure Termali)**			**Previsto ma non pianificato per il 2011**	

Assistenza sanitaria di base	**B (Medicina di base: generale e pediatrica)**			**Non previsto**	B contiene i dati extra ASL proveneinte dalla Regione o altre regioni. Scelta:Rapporto Soggetto / Medico sarebbe AURA. Una volta con AURA live su tutte le aziende, il flusso B andrebbe a morire
		AURA	DWH – AURA	Settembre 2011 conclusa la migrazione a front end PADDI BOXI	
Riconoscimento del diritto all'esenzione		AURA			
?		Diabetici	DWH Diabetici	**Esistente**	
Programmi di diagnosi precoce		Screening Tumori Femminili		Non **prevista un'evolutiva verso DWH PADDI**	**Esiste DWH Settoriale** DWH Screening Tumori Femminili
		Screening Colon Retto		Non **prevista un'evolutiva verso DWH PADDI**	**Esiste DWH Settoriale** DWH Screening Colon Retto
?		Emodinamica	DWH Emodinamica	**Sospesa** e da ripianificare	(per mancanza dati alla fonte)
Accertamenti di invalidità civile, disabilità, handicap		PABI/Medicina Legale		**Da valutare** attività evolutiva verso DWH PADDI	**Esiste DWH Settoriale** DWH-PABI/Medicina Legale.
Malattie infettive e diffusive		Malattie Rare		**E' Pianificata un'evolutiva verso PADDI entro l'anno 2011**	**Esiste DWH Settoriale** DWH-Malattie rare.
Dipendenze		SPIDI		**E' Pianificata un'evolutiva verso PADDI entro l'anno 2011**	**Esiste DWH Settoriale** DWH-SPIDI.
Certificati di assistenza al parto ed esiti gravidanza		CEDAP (certificato d'assistenza al parto)	DWH CEDAP	**Esistente**	
Attività fisica e sportiva		Medicina Sportiva		**Non previsto**	
Assistenza integrativa		Protes		**E' Pianificata un'evolutiva verso PADDI entro l'anno 2011**	**Esiste DWH Settoriale** DWH-Protes
Rischi infortunistici e sanitari connessi con		Spresal		**Non prevista**	

Archivi Dati da Scheda 12	Flusso di riferimento	DB Operazionale di riferimento	Componente DWH PADDI	Stato	Note
gli ambienti di vita e di lavoro					
Infortuni stradali	**n.a.**	n.a.	n.a.	n.a.	
Indagini di soddisfazione degli utenti	**n.a.**	n.a.	n.a.	n.a.	
Dati sulla mortalità presso le aziende ASL			DWH SDO (Schede Dimissione Ospedaliere)	Esistente (DWH SDO)	
Assistenza psichiatrica	**n.a.**	n.a.	n.a.	n.a.	
Vaccinazioni		PASTEUR	n.a.	n.a.	

1.1.2 I volumi dei flussi sanitari

A supporto dell'analisi svolta per definire l'infrastruttura del Sistema di Anonimizzazione Reversibile è stata effettuata una stima dei volumi dei diversi Flussi Regionali, per anno e per posizioni anagrafiche, le cui evidenze vengono di seguito riportate.
Per i Flussi sui quali è stato possibile si è applicata la regola dell'uguaglianza delle 6 informazioni anagrafiche:

1. Nome
2. Cognome
3. Data di Nascita
4. Comune di Nascita
5. Sesso
6. Codice Fiscale

Dove invece ciò non è stato possibile si è applicata la sola regola di uguaglianza del Codice Fiscale.

Di seguito viene riportata la tabella contenente il numero dei volumi stimati per anno e per tipo di flusso.

Per il Flusso C, viene riportato il conteggio dei record anagrafici, eseguito con "distinct" su Codice Fiscale ed escludendo i record con CF non univoco (tutti 9, 'STP9999999999999','ENI9999999999999', tutti zero) che sono stati evidenziati a parte:

Conteggio record Anagrafici per flusso e anno di competenza 03/12/2010
Il conteggio è riferito alla situazione consolidata alla chiusura della competenza

	Totale record									
Flusso	**2009**	**2008**	**2007**	**2006**	**2005**	**2004**	**2003**	**2002**	**2001**	**2000**
SDO	860.794	864.862	825.276	822.209	811.069	812.383	789.498	797.935	818.058	835.526
B	405.648	378.992	387.262	378.303	361.813	345.795	321.400	264.088	244.328	164.763
C	22.864.272	22.033.537	21.013.146	20.134.492	19.551.878	18.523.070	17.089.139			
C2	1.850.358	1.801.114	1.678.628	1.795.439	1.559.544	1.411.407	1.410.271			
C5	860.430	972.768	1.032.027	739.554	676.488	275.191	246.559	254.678		
D	1.789.631	1.665.971	1.847.479	1.703.134	1.618.391	1.711.799	1.557.094	1.491.634	1.401.988	2.403.974
E	26.383	26.174	27.193	27.092	27.105	26.648	26.046	25.946	25.440	20.600
F	1.320.882	1.064.742	912.988	672.655	591.759	516.703	260.131	118.297	75.007	42.773

Conteggio con distinct su : Codice Fiscale, Cognome, Nome, Sesso, Data di nascita, Comune di nascita

	2009	**2008**	**2007**	**2006**	**2005**	**2004**	**2003**	**2002**	**2001**	**2000**
Flusso SDO	577.409	597.573	598.127	596.853	587.393	590.432	576.502	576.566	589.124	598.293
	67%	69%	72%	73%	72%	73%	73%	72%	72%	72%

Figura 2 - Fonte: Elaborazioni CSI-Piemonte su dati flussi regionali (Dic. 2010)

Mese competenza	Num. rec.
2009/01	60.383
2009/02	63.295
2009/03	69.981
2009/04	65.083
2009/05	65.092
2009/06	61.690
2009/07	62.415
2009/08	43.451
2009/09	58.931
2009/10	65.572
2009/11	63.001
2009/12	66.181

Anno	Num. rec	Num. rec con CF non univoco
2009	3.270.688	380.981
2008	3.261.813	426.373
2007	3.217.135	461.591
2006	3.219.889	351.195
2005	3.195.606	357.150
2004	3.106.381	296.985
2003	2.998.545	229.977

Figura 3 Fonte: Elaborazioni CSI-Piemonte su dati flussi regionali (Dic. 2010)

Per il flusso SDO, viene riportato il conteggio dei record anagrafici, eseguito con distinct su : Codice Fiscale, Cognome, Nome, Sesso, Data di nascita e Comune di nascita - suddivisione per Mese di competenza (Mese di dimissione della SDO)

6 Assunzioni "organizzative e di processo"

6.1 La "*bruciatura*" del codice anonimo

Con il termine "*bruciatura codice anonimo*" s'intende l'evenienza di situazioni in cui risulti possibile, tramite elaborazioni statistiche, risalire all'associazione tra i dati identificativi diretti della persona ed il codice anonimo "muto" utilizzato dal sistema di anonimizzazione, rendendo non sicuro l'utilizzo di quel codice per il futuro.
Il sistema non prevede alcun meccanismo di rigenerazione del codice anonimo, qualora si verifichi un evento di "*bruciatura*".
Non essendo possibile prevenire e/o risolvere tecnicamente l'eventuale "bruciatura" di codici anonimi, **è necessario ricorrere a regole ed a processi organizzativi di trattamento dei dati capaci di prevenire la bruciatura dei codici.**

6.2 Le regole di sistema

PRESCRIZIONI ALL'USO DEI DATI

Uno stesso Ente può svolgere attività di trattamento dati sanitari per finalità diverse:

- **Attività trattamento dati sanitari anonimi per finalità scheda 12**: programmazione, controllo e valutazione dell'assistenza sanitaria (Prescrizioni all'uso dei dati per scopi statistici e scientifici All. A4 D.Lgs 196/2003);
- **Attività trattamento dati sanitari in chiaro per fini di prevenzione, diagnosi, cura e riabilitazione:** artt. 75-84 D.Lgs. 196/2003;
- **Attività trattamento dati sanitari in chiaro per fini di ricerca scientifica**: art. 12/bis D.L. 502/92, art. 110 D.Lgs196/2003;
- **Attività trattamento dati sanitari in chiaro legato ai registri di patologia istituiti con legge nazionale o regionale** (art. 94 D.Lgs196/2003)
- **Altre Attività trattamento dati sanitari in chiaro in attuazione di specifiche norme** che disciplinano l'attività, individuando i dati trattati e le operazioni effettuate (registri di patologia istituiti con legge).

Uno stesso Ente/Servizio può disporre degli stessi dati sanitari in diversi trattamenti (anonimi ed in chiaro), in tal caso è necessario il rispetto delle prescrizioni all'uso dei dati redatte da Regione Piemonte nell'ambito dell'utilizzo del sistema di anonimizzazione, per favorire il rispetto dei **principi di pertinenza e non eccedenza nel trattamento dei dati** e delle misure di sicurezza (ai sensi dell'art. 106 D. Lgs. 196/2003).

LA TECNICA DEL POS (Point of Service bancario)

Chi elabora il dato anonimo non deve conoscere il dato in chiaro "*reversato*" e viceversa. Questa regola determina le condizioni organizzative utili ad assicurare il controllo del sistema (evitando così eventuali "bruciature") ed il governo delle informazioni trattate (pertinenza e non eccedenza).

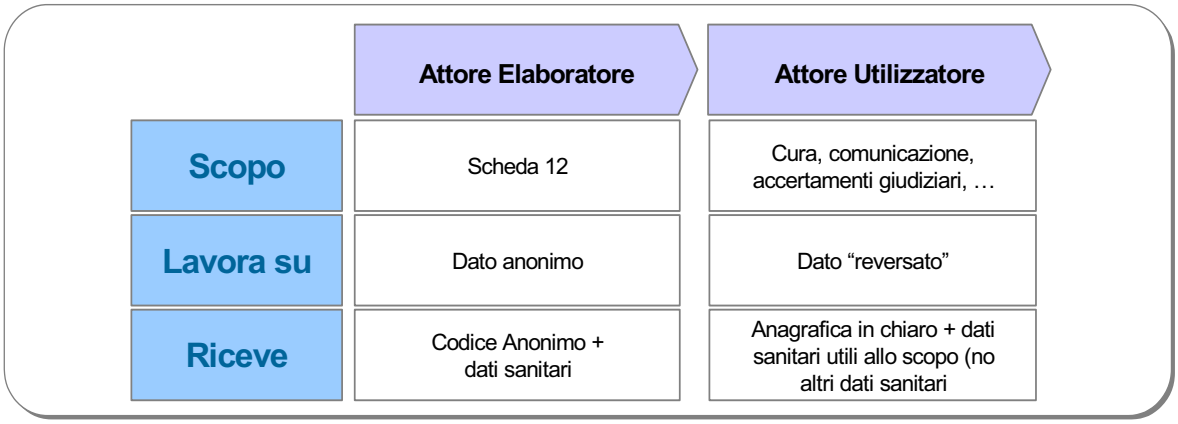

Figura 4 - L'utilizzo dati sanitari: anonimi ed in chiaro

ASSUNZIONI DERIVATE DALLA TECNICA POS

• Il **Fruitore del dato in chiaro** non deve conoscere i dati caratterizzanti le singole prestazioni sanitarie oggetto di attività scheda 12.

• Il **Fruitore del dato anonimo** non deve conoscere i dati identificativi in chiaro degli assistiti.

• Solo la **Struttura Tecnica** ha la possibilità di associare l'identificativo anonimo ed il dato anagrafico in chiaro, previa autorizzazione e tramite procedura automatizzata resa sicura da opportuni protocolli.

CONSEGUENZA DERIVATE DALLA TECNICA POS

• Il **Fruitore dato anonimo** non deve mai disporre dei dati “in chiaro”, anche di titolarità di un terzo fornitore, nell’ambito di attività di programmazione e di controllo (scheda 12).

• Il **Fornitore Esterno** deve inviare i dati in chiaro alla **S.R. Anonimizzazione** o alla **Struttura Tecnica.**

• I dati provenienti dal **Fornitore Esterno** devono essere anonimizzati (id temporaneo) dalla **Struttura Tecnica** prima di essere inviati al **Fruitore dato anonimo.**

.

6.3 Regole Generali

Sono di seguito esposte le regole organizzative generali da attuare a partire dal momento in cui sarà reso operativo il "Sistema di Anonimizzazione" e sarà attivata la funzione di Anonimizzazione regionale in seno al competente settore.

SCARICO DATI ANONIMI

⟶ ***Richiesta***

Un Richiedente dato anonimo che necessita di uno o più scarichi dati anonimi deve essere preventivamente autorizzato dalla S.R. Anonimizzazione.

Il Richiedente dato anonimo dovrà indicare e motivare la finalità del trattamento dati anonimi.

⟶ **Autorizzazione**

La S.R. Anonimizzazione, all'avvio del sistema, fornirà a tutti gli **Enti citati in Scheda 12 un'autorizzazione permanente** allo scarico dati anonimi per finalità Scheda 12.

La S.R. Anonimizzazione può fornire ad un richiedente **Ente non citato in Scheda 12** solo **autorizzazioni temporanee** allo scarico dati anonimi. La specifica nota autorizzativa "temporanea" dovrà riportare anche il dettaglio delle informazioni da rendere disponibili.

⟶ ***Anonimizzazione***

Lo scarico di dati anonimi per fruitori **Enti citati in Scheda 12** prevede codici anonimi **standard**.

Lo scarico di dati anonimi per fruitori **Enti non citati in Scheda 12** prevede codici anonimi **temporanei.**

La struttura tecnica che effettua il servizio di anonimizzazione non traccia il motivo (finalità) dello scarico ma solo gli estremi della specifica nota autorizzativa regionale.

⟶ ***Strumenti ed Oneri Economici***

Il Fruitore di dati anonimi utilizzerà il DWH Salute (PADDI) per accedere ai dati aggregati tramite la reportistica disponibile. Eventuali costi per richieste di nuova reportistica dovranno essere valutati puntualmente e saranno a carico del richiedente/fruitore.

Il Fruitore di dati anonimi utilizzerà lo strumento SDS per lo scarico dei dati anonimi. Eventuali costi di elaborazione e di estrazione/consegna sono a carico del richiedente.

ANONIMIZZAZIONE FONTE DATI ESTERNA

⟶ ***Richiesta***

Un Ente citato in Scheda 12, che ha la necessità di correlare una fonte esterna in chiaro (titolarità di un soggetto terzo "Fornitore Esterno") ai dati sanitari "anonimi" presenti nel DWH sanitario regionale, deve richiedere autorizzazione alla S.R. Anonimizzazione, indicando e motivando la finalità del trattamento dati e specificando il nominativo ed i contatti del fornitore esterno.

⟶ ***Autorizzazione***

In generale l'anonimizzazione di fonte dati esterne non è ammessa,

La S.R. Anonimizzazione deve valutare la singola richiesta nel rispetto:

- della normativa (artt. 39 e 110 del D.Lgs 196/2003);
- della regola del POS (Bruciatura);
- delle prescrizioni all'uso dei dati e del codice deontologico (rif. All. A4 del D.Lgs 196/2003).

La S.R. Anonimizzazione autorizza o meno l'anonimizzazione della fonte esterna, comunicando contestualmente al richiedente, in caso di autorizzazione, la necessità che il fornitore esterno provveda a nominare la Struttura Tecnica quale Responsabile Esterno al trattamento dei dati in chiaro contenuti nell'archivio da anonimizzare.

⟶ ***Anonimizzazione***

Il Fornitore esterno deve nominare la Struttura Tecnica quale Responsabile Esterno al trattamento dei dati, procedendo poi alla consegna dell'archivio dei dati in chiaro attraverso l'utilizzo di strumenti informatici "sicuri".

L'anonimizzazione di una fonte esterna **prevede sempre l'assegnazione di un codice anonimo temporaneo.**

Lo scarico dei dati anonimi sanitari, di cui era stata richiesta la correlazione con la fonte dati esterna, deve essere consistente, ossia essere generato assegnando gli stessi codici anonimi temporanei utilizzati per l'anonimizzazione della fonte esterna.

⟶ ***Strumenti ed Oneri Economici***

Lo strumento da utilizzarsi per l'acquisizione, l'archiviazione, la tracciatura e l'elaborazione dell'archivio dati in chiaro, di titolarità di un terzo fornitore, sarà gestito dalla Struttura Tecnica in modalità "sicura" , adottando gli opportuni protocolli. Nel caso di Fruitori in rete RUPAR, questi utilizzeranno SDS quale strumento per lo scarico massivo dei dati anonimi (anche quelli eventualmente prodotti dall'anonimizzazione di una fonte esterna). Nel caso di Fruitori non in rete RUPAR, questi dovranno concordare con la Struttura Tecnica specifiche modalità di interscambio.

Eventuali costi di elaborazione e di estrazione/consegna sono a carico del richiedente.

Punti di riflessione – Anonimizzazione Fonte Dati Esterna

1) L'Ente richiedente deve comunicare al fornitore esterno la necessità che questi provveda a nominare la Struttura Tecnica quale Responsabile Esterno al trattamento dei dati in chiaro presenti nella fonte esterna.
2) Il fornitore esterno, dopo aver nominato la Struttura Tecnica quale Responsabile Esterno al trattamento dei dati, consegna i dati in chiaro direttamente alla Struttura Tecnica in modalità "sicura".

Lo stesso vale anche nel caso in cui l'Ente Richiedente sia anche il Fornitore dei dati esterni:

- Prima l'Ente nomina la Struttura Tecnica come Responsabile Esterno al trattamento dei dati in chiaro.
- Poi procede all'invio/consegna dei dati direttamente alla Struttura Tecnica, sempre in modalità "sicura".

REVERSIBILITA'

⟶ ***Richiesta***

Un Richiedente/Fruitore di dati in chiaro, che necessita dei ottenere la reversibilità di uno o più codici anonimi, richiede autorizzazione alla S.R. Anonimizzazione.

Il Richiedente/Fruitore dei dati in chiaro indicherà il motivo della reversibilità ed il riferimento della richiesta di scarico dei dati anonimi (estremi della nota autorizzativa), riferita all'attività dalla quale è poi emersa l'esigenza di fruire dei dati in chiaro.

⟶ ***Autorizzazione***

La S.R. Anonimizzazione **valuta** la richiesta nel rispetto:

- della normativa (artt. 39 e 110 del D.Lgs 196/2003);
- della regola del POS (Bruciatura)
- delle prescrizioni all'uso dei dati e del codice deontologico (rif. All. A4 del D.Lgs 196/2003)

La S.R. Anonimizzazione ha la responsabilità di autorizzare o meno la reversibilità dei dati sanitari "anonimi" di competenza regionale (scheda 12).
Nel caso specifico del richiedente "*Autorità Giudiziaria*" l'autorizzazione sarà sempre concessa in presenza di richiesta formale.

⟶ ***Reversibilità***

La Struttura Tecnica elabora la reversibilità dei dati anonimi standard.
La reversibilità dei dati anonimi temporanei è ammessa, previa autorizzazione, solo per gli Enti Scheda 12, nonché per l'Autorità Giudiziaria.
La Struttura Tecnica non traccia il motivo (finalità) della reversibilità ma solo il riferimento alla nota autorizzativa.

⟶ ***Strumenti ed Oneri Economici***

Le modalità di consegna degli scarichi dati in chiaro "reversati" dovranno essere concordate tra il fruitore e la struttura tecnica.

I costi delle singole richieste rientreranno tra quelli di gestione del servizio annuale di Anonimizzazione.

Punti di riflessione – Reversibilità

- La reversibilità non è prevista per gli Scarichi Anonimi con ID temporaneo verso Enti Fruitori non citati in Scheda 12.
- La reversibilità non è prevista per gli scarichi dati anonimi con anonimizzazione di una fonte esterna (non presente nel DWH Sanitario Regionale).

In generale, la reversibilità non è consentita per tutti gli scarichi di dati anonimi con identificativi temporanei (fatta eccezione per richieste provenienti dall'Autorità giudiziaria).

7 Atti Organizzativi e strumenti

7.1 Atti organizzativi: Istituzione di una funzione per la gestione dell'Anonimizzazione

Si dovrà rendere operativa, presso una struttura regionale, la funzione Anonimizzazione per sovrintendere alle attività da svolgersi nell'ambito dei seguenti 3 macroprocessi:

- **Scarico Dati Anonimi:**
  - Predisposizione, all'avvio del sistema, a favore di tutti gli Enti citati in Scheda 12, apposita nota di autorizzazione permanente allo scarico dei dati anonimi per trattamenti con finalità Scheda 12.
  - Valutazione/Concessione di autorizzazioni temporanee a fronte di specifiche richieste da parte di Enti non citati in Scheda 12.
  - Interfaccia con la Struttura Tecnica per le richieste di scarico di dati anonimi.

- **Reversibilità**
  - Valutazione/autorizzazione delle richieste di reversibilità (autorizzazione sempre concessa all'Autorità Giudiziaria).
  - Interfaccia con la Struttura Tecnica per consentire la reversibilità.

- **Anonimizzazione**
  - Valutazione/autorizzazione delle richieste di anonimizzazione fonti dati esterne.
  - Interfaccia con la Struttura Tecnica per consentire l'anonimizzazione temporanea. (La Struttura Tecnica dovrà essere nominata dal Fornitore Esterno quale Responsabile Esterno al Trattamento dei dati.

7.2 Atti Organizzativi – Autorizzazione Scarichi Dati Anonimi

Tutti gli accessi al Patrimonio Informativo Sanitario Anonimizzato (DWH Sanitario Regionale) dovranno essere autorizzati. Le autorizzazioni sono:

- Per singola richiesta → ***Provvedimento Regionale di autorizzazione temporanea***
- "Permanenti" solo per gli Enti che hanno compiti istituzionali di supporto, programmazione e valutazione di servizi sanitari (citati in Scheda 12) e limitatamente al loro ambito di competenza (trattamento per finalità Scheda 12) → ***Provvedimento Regionale di autorizzazione permanente.***

7.3 Atti Organizzativi – Autorizzazione Reversibilità

Tutti gli Enti/Servizi che richiederanno la reversibilità del dato sanitario anonimo dovranno essere autorizzati dalla S.R. Anonimizzazione.
L'autorizzazione sarà sempre per singola richiesta → Provvedimento Regionale di autorizzazione temporanea.
Nel caso in cui la richiesta provenga dall'autorità giudiziaria, questa è da ritenersi automaticamente accolta.
In tutti gli altri casi, il Gruppo di Lavoro a supporto dell'attuazione del Progetto "Realizzazione del Sistema di Anonimizzazione Reversibile del patrimonio informativo sanitario", istituito con D.D. n. 1071 del 17 dicembre 2010, dovrà predisporre specifico parere, cui il competente Settore regionale farà riferimento per il relativo accoglimento o diniego dell'istanza di reversibilità.

7.4 Atti Organizzativi - Prescrizioni all'uso dei dati ed autorizzazione per Struttura Tecnica

La modulistica prevista all'interno del processo autorizzativo, presidiato dalla S.R. Anonimizzazione, dovrà contenere le prescrizioni all'uso dei dati al fine di evitare:

- elaborazioni finalizzate alla ricostruzione del dato in chiaro;
- la diffusione dei dati ricevuti in formato anonimo/in chiaro.

7.5 Atti Organizzativi – Proposta su Modulistica Funzione regionale Anonimizzazione

Schema del Provvedimento Autorizzativo Permanente per scarico dati anonimi standard:

- Contiene le indicazioni sulle prescrizioni all'uso dei dati (con i richiami alla pertinenza e non eccedenza prevista nel D.Lgs 196/2003)

- Viene adottato e trasmesso a tutti gli Enti citati in scheda 12 all'avvio del sistema di anonimizzazione reversibile.

Modulo Richiesta/Autorizzazione Scarico Dati Anonimi (solo Autorizzazione Temporanea)

- Contiene le indicazioni sulle prescrizioni all'uso dei dati (con i richiami alla pertinenza e non eccedenza prevista nel D.Lgs 196/2003)
- Viene compilato solo dagli Enti Richiedenti non citati in scheda 12
    - Indica il motivo del trattamento
    - Allega specifiche tecniche per il singolo scarico, con le indicazioni puntuali sulle informazioni da rendere disponibili

Modulo Richiesta Scarico Dati con anonimizzazione Fonte Dati Esterni

- Contiene le indicazioni sulle prescrizioni all'uso dei dati (con i richiami alla pertinenza e non eccedenza prevista nel D.Lgs 196/2003)
- Indica l'Ente richiedente (solo per enti citati scheda 12)
- Indica il motivo del trattamento
- Indica l'Archivio Dati Esterno da anonimizzare:
    - Titolare Archivio (Fornitore Esterno)
    - Contenuto Archivio
- Allega le specifiche tecniche per lo scarico e per la fonte dati da anonimizzare

Modulo Richiesta Reversibilità

- Riferimento alla richiesta di scarico di dati anonimi con ID standard/Temporaneo, dalla cui disponibilità è sorta l'esigenza di richiedere la reversibilità
- Indica il motivo della reversibilità: finalità cura, assistenza, controllo giudiziario
- Riporta l'elenco degli ID anonimi
- Indica chi deve essere il Fruitore/i dei dati in chiaro ("reversati")

7.6 Gli strumenti

Con l'avvio del Sistema Anonimizzazione il Patrimonio Informativo Sanitario Anonimizzato è costituito dal contenuto del DWH Sanitario Regionale.
In particolare, gli strumenti utilizzati per la sua fruizione sono:

- **PADDI-DWH Salute**: per estrazione di reportistica (dati aggregati)
- **SDS - Scarico Dati Salute** :
  - per lo scarico massivo di dati anonimi di dettaglio
  - per lo scarico di dettaglio anonimo di archivi esterni (di titolarità di un terzo Fornitore)
- **RS Reversibilità Dati Salute**:
  - per lo scarico dei dati anonimi standard "reversati"

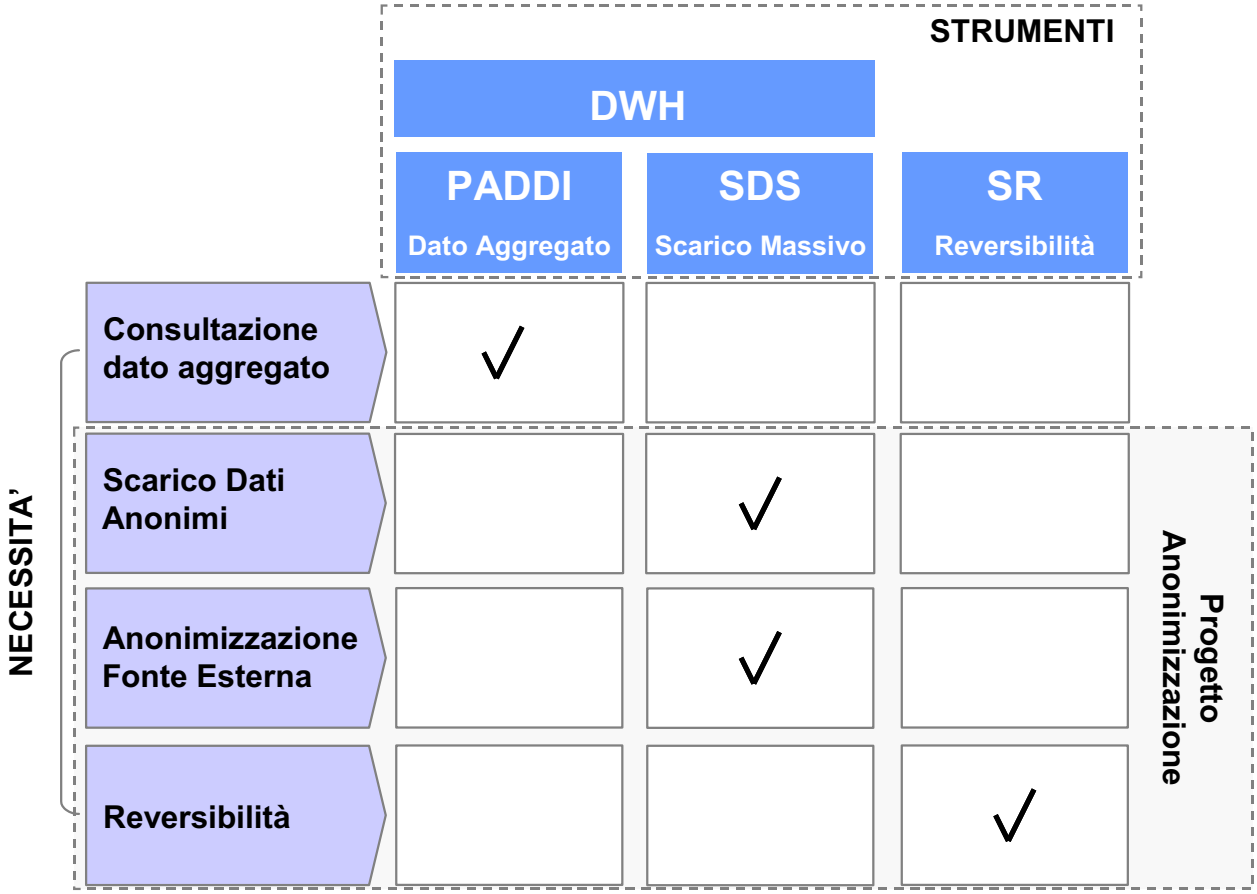

Figura 5 - Strumenti

IDENTIFICATIVI ANONIMI

Il Sistema Anonimizzazione reversibile dei dati sanitari prevede l'anonimizzazione standard e quella temporanea, attraverso la generazione di:

- ID anonimo originale
- ID anonimo per CF
- ID anonimo ricondotto
- ISL

	Anonimizzazione Standard		Anonimizzazione Temporanea	
Id Anonimo Originale	*Calcolato sui campi Codice Fiscale, Cognome, Nome, Genere, Data Nascita e Luogo di Nascita presenti nel "record". Assume valori numerici interi positivi in base dieci*	*12542*	*Associato ad un id anonimo Originale standard. Un id anonimo temporaneo sarà associato ad un id anonimo standard una ed una sola volta. E' composto da un numero esadecimale di 16 cifre*	*000000000003D61D*
Id Anonimo CF	*Calcolato solo sul campo Codice Fiscale, presente nel "record". Potrebbe coincidere con Id Anonimo Originale. Assume valori numerici interi positivi in base dieci*	*20452*	*Associato ad un id anonimo CF standard. Un id anonimo temporaneo sarà associato ad un id anonimo standard una ed una sola volta. E' composto da un numero esadecimale di 16 cifre*	*00000000000499D4*
Id Anonimo Ricondotto	*E' l'identificativo anonimo dell'assistito a cui è stato ricondotto un soggetto presente in un record. Potrebbe coincidere con Id Anonimo Originale Assume valori numerici positivi interi in base dieci*	*10748*	*Associato ad un id anonimo Ricondotto standard. Un id anonimo temporaneo sarà associato ad un id anonimo standard una ed una sola volta. E' composto da un numero esadecimale di 16 cifre*	*000000000003AF74*
ISL	*Indicatore Sintetico del Linkage, rappresenta (una lettera) la classe di affidabilità del legame tra soggetto originale e soggetto ricondotto*	*B*	*Coincide con ISL della Anonimizzazione Standard*	*B*

Figura 6 - Identificativi Anonimi

8 Il Macroprocesso di riferimento

Di seguito è rappresentato il macroprocesso di riferimento che illustra le attività che devono essere svolte dal momento dell'acquisizione del dato in chiaro alla messa a disposizione del dato anonimo, nelle forme e modalità previste per assicurare, nei limiti delle possibilità, l'integrità del sistema (non bruciatura dei codice anonimo).

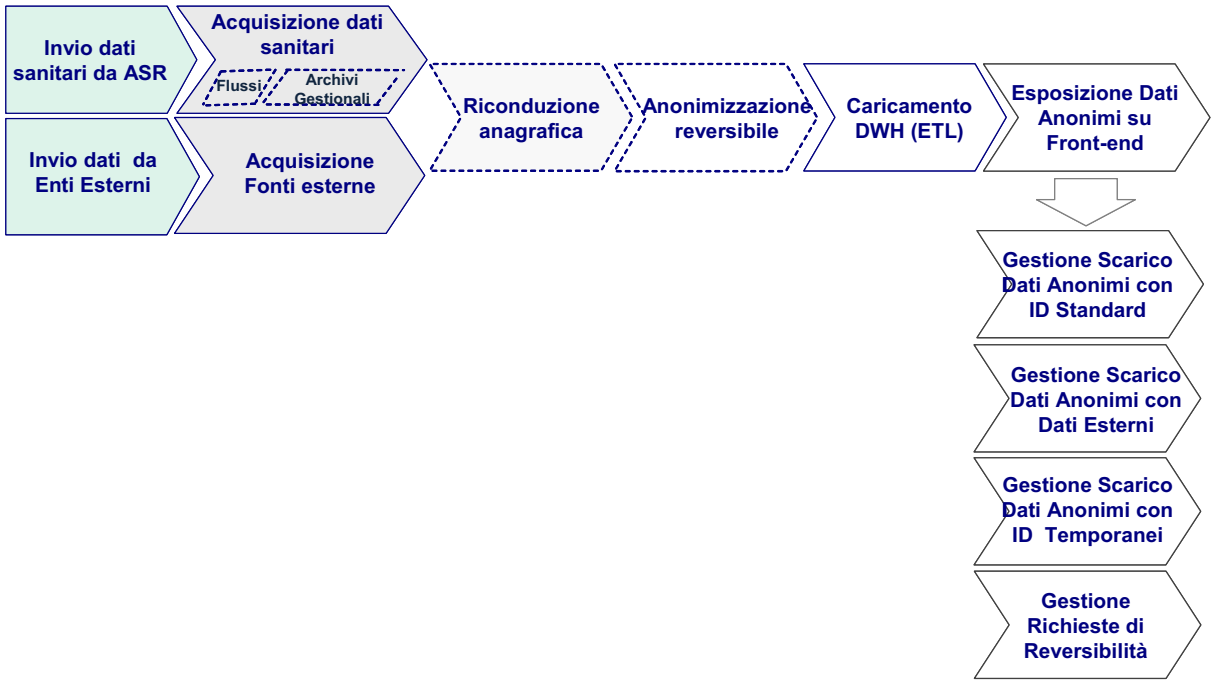

Figura 7-I macroprocessi