

Garante per la protezione dei dati personali
Sistema informativo per le dipendenze e privacy

Il Garante per la protezione dei dati personali, nella riunione odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Mauro Paissan e del dott. Giuseppe Fortunato, componenti e del dott. Filippo Patroni Griffi, segretario generale;

Vista la richiesta di parere del Ministero del lavoro, della salute e delle politiche sociali;

Visto l'art. 154, commi 4 e 5, del Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196); Vista la documentazione in atti; Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Giuseppe Fortunato;

Premesso:

Il Ministero del lavoro, della salute e delle politiche sociali ha chiesto il parere del Garante in ordine a uno schema di decreto recante l'istituzione del sistema informativo per le dipendenze (di seguito indicato come Sind).

Il decreto riguarda interventi sanitari e socio sanitari erogati da operatori del Servizio sanitario nazionale nell'ambito dell'assistenza rivolta alle persone dipendenti da sostanze stupefacenti o psicotrope o da alcool.

Il presente parere si riferisce a una versione dello schema che tiene conto di alcune osservazioni svolte nell'ambito di incontri tecnici tenutisi presso questa Autorità.

Osserva:

1. Le finalità del sistema

Lo schema di decreto prevede che il Sistema informativo nazionale dipendenze, istituito nell'ambito del Nuovo Sistema informativo sanitario (NSIS) presso il Ministero del lavoro, della salute e delle politiche sociali, è il sistema di supporto al conseguimento delle finalità definite nel decreto. Attraverso le sue funzionalità le Regioni e le Province autonome mettono a disposizione del predetto NSIS informazioni relative a strutture, attività e personale dei servizi delle dipendenze, al fine di consentirne un'adeguata analisi a livello nazionale e regionale.

I dati oggetto dei flussi informativi, le modalità di alimentazione del sistema informativo e le sue caratteristiche tecniche sono specificati nel disciplinare tecnico allegato al decreto.

Per assicurare il rispetto del principio di finalità (art. 11, comma 1, lett. b) del Codice in materia di protezione dei dati personali) è necessario che le finalità per le quali i dati devono essere raccolti nel SIND e che si intendono perseguire mediante il sistema siano indicate espressamente e in maniera esaustiva nell'articolato del decreto.

Allo stato, invece, indicazioni circa le possibili finalità cui è preordinato il sistema sono contenute solo nel preambolo e nel disciplinare tecnico allegato allo schema (parr. 1 e 3.5. disc. tecn.) e in maniera, peraltro, non esaustiva come può dedursi dall'uso delle locuzioni "fra l'altro" e "principali" cui, rispettivamente, si fa ricorso.

2. Dati non direttamente identificativi degli interessati

Il Ministero del lavoro, della salute e delle politiche sociali, nonché le Regioni e le Province autonome possono trattare dati personali sensibili, anche idonei a rivelare lo stato di salute, per finalità che rientrano nei compiti del Servizio sanitario nazionale. In particolare, possono essere trattati dati per attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria (art. 85, comma 1, lett. b) del Codice) purché non direttamente identificativi degli interessati (art. 20, comma 3, del Codice; d.m. 12 dicembre 2007, n. 277, all. n. C-01; scheda 12

dello schema tipo di regolamento per il trattamento dei dati sensibili e giudiziari delle regioni e delle province autonome approvato dal Garante con parere del 13 aprile 2007).

Per dare attuazione a tale cornice normativa, lo schema di decreto precisa che il contesto dei dati trattati mediante il SIND è costituito da “informazioni individuali ma non nominative” (art. 2, comma 2, dello schema; par. 3.1 disc. tecn.).

Inoltre, per garantire la non identificabilità diretta delle persone i cui dati sono trattati nell’ambito del SIND, a ciascun soggetto è assegnato un codice univoco (cfr. art. 5, comma 3, dello schema). Tale misura è stabilita in applicazione di quanto previsto dai predetti regolamenti, a norma dei quali i dati raccolti e comunicati dalle aziende sanitarie all’amministrazione regionale di riferimento sono privati degli elementi identificativi diretti (come, ad esempio, il nome e il cognome del paziente) subito dopo la loro acquisizione da parte della regione e a ciascun soggetto è assegnato, appunto, un codice univoco.

Lo schema prevede anche, opportunamente, che il codice assegnato deve essere diverso da analogo codice utilizzato nella trasmissione dei dati di altri sistemi informativi, per non consentire l’interconnessione con altre banche dati (art. 5, comma 3, dello schema).

L’Autorità prende atto favorevolmente di tali previsioni e ritiene necessario, sul piano formale, sostituire, ovunque ricorra, la locuzione “informazioni individuali ma non nominative” con quella, più corretta, di “dati personali non identificativi” (art. 4, comma 1, lett. c) del Codice).

Inoltre, è necessario completare le garanzie per gli interessati prevedendo, in conformità a quanto stabilito nella scheda 12 del regolamento citato, che le regioni e le province autonome che non dispongono di sistemi di codifica utilizzino solo dati anonimi (analogia integrazione deve essere apportata nel preambolo laddove si riporta il contenuto della scheda 12).

3. L’accesso ai dati e il loro utilizzo

Per assicurare il rispetto dei principi di proporzionalità e di indispensabilità nel trattamento dei dati sensibili lo schema deve essere integrato con mirate disposizioni che assicurino l’accesso selettivo alle informazioni conservate nel sistema ed il loro utilizzo proporzionato rispetto alle finalità perseguite.

In particolare, si ritiene necessario:

a) individuare specificamente, nell’articolato, le unità organizzative del ministero, delle regioni e delle province ai cui addetti è consentito il trattamento delle informazioni del SIND, anche mediante l’indicazione delle specifiche attribuzioni ad esse assegnate (cfr., invece, il paragrafo 3.1 del disciplinare tecnico ove si fa riferimento genericamente agli “uffici regionali preposti” e “agli uffici del livello nazionale”);

b) specificare nell’articolato, piuttosto che nel disciplinare tecnico (cfr. par. 3.5), che il ministero può accedere all’insieme delle informazioni raccolte nell’ambito del SIND, mentre le regioni e le province autonome possono trattare solo le informazioni da esse stesse inserite;

c) assicurare l’accesso selettivo alle informazioni, evitando, in particolare, la consultazione di dati riferiti a singoli individui e favorire la rappresentazione aggregata delle informazioni. A tale scopo lo schema potrebbe essere integrato con le disposizioni che si suggeriscono o con altre di analogo tenore: “Nel SIND sono raccolti e trattati solo i dati indispensabili per lo svolgimento di elaborazioni statistiche, ricerche, studi e analisi necessari per il perseguimento delle finalità del presente decreto, con modalità e logiche di organizzazione ed elaborazione delle informazioni dirette esclusivamente a fornire una rappresentazione aggregata dei dati. Gli incaricati del trattamento possono accedere ai dati registrati nel SIND soltanto per singole chiavi di ricerca che non devono consentire, anche mediante operazioni di interconnessione e raffronto, la consultazione, la selezione o l’estrazione di informazioni riferite a singoli individui o di elenchi di codici identificativi. Le funzioni applicative del sistema non devono consentire la consultazione e l’analisi di informazioni che rendano identificabile l’interessato ai sensi dei codici di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici o scientifici di cui agli allegati A3 e A4 del decreto legislativo 30 giugno 2003, n. 196.”.

4. Anonimato

L'articolo 120 del testo unico delle leggi in materia di tossicodipendenze (d.P.R. n. 309/1990) prevede che chiunque si sottoponga ad un programma terapeutico e socio-riabilitativo possa richiedere l'anonimato nei rapporti con i servizi e gli altri presidi sanitari competenti. In tal caso, tali persone hanno diritto a che la loro scheda sanitaria non contenga le generalità né altri dati che valgano alla loro identificazione.

L'Autorità prende atto che lo schema di decreto richiama espressamente il diritto all'anonimato (art. 5, comma 2, dello schema). Per assicurare il rispetto di tale diritto, peraltro, è necessario che nel disciplinare tecnico cui la norma fa rinvio sia specificato che, in tali casi, non devono essere comunicati dati riferiti agli interessati, indicati nel flusso relativo all'attività (par. 5.3. disc. tecn.), diversi da quelli relativi al codice regione, all'anno di nascita, al sesso e al tipo di trattamento (par. 5.3.1 disc. tecn.).

5. Il principio di proporzionalità e il trattamento di dati particolari

5.1. La particolare delicatezza dei dati trattati nell'ambito del SIND ne impone, come abbiamo già sottolineato, un utilizzo proporzionato rispetto alle finalità perseguite. Si richiama, pertanto, l'attenzione delle amministrazioni interessate sulla necessità di valutare, in concreto, se le singole informazioni elencate nel disciplinare tecnico, oggetto di trattamento nel SIND, siano effettivamente pertinenti e non eccedenti nonché indispensabili rispetto alle finalità del decreto.

5.2. L'articolo 5 della legge 5 giugno 1990, n. 135, in materia di lotta contro l'AIDS prevede che in caso di infezioni da HIV l'operatore sanitario che ne viene a conoscenza deve adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato. Inoltre, la rilevazione statistica di tale infezione deve essere effettuata con modalità che non consentano l'identificazione della persona e l'accertamento della sindrome è consentito, nell'ambito di programmi epidemiologici, solo quando i campioni da analizzare siano stati resi anonimi con assoluta impossibilità di pervenire all'identificazione delle persone interessate.

In base a tale quadro normativo e alle garanzie previste, l'anonimato della persona è obbligatorio per legge e non rimesso ad una eventuale richiesta dell'interessato. Pertanto, poiché le modalità di trattamento dei dati previste dal decreto non forniscono garanzie adeguate ad assicurare pienamente il rispetto dell'anonimato, non può ritenersi, allo stato, consentita la raccolta nell'ambito del SIND di informazioni personali attinenti a tale infezione, e ogni previsione in tal senso dovrà quindi essere espunta dal disciplinare tecnico allegato al decreto (par. 5.3.2; par. 5.3.5. "Codice farmaco" n. 14, disc. tecn.).

5.3. Per rispettare il principio di proporzionalità nel trattamento dei dati si rimette alla ponderata valutazione dell'amministrazione l'opportunità di prevedere la raccolta nel SIND di soli gruppi di patologie concomitanti con lo stato di dipendenza dell'interessato, e non delle singole patologie indicate nell'elenco dettagliato di cui al dizionario ICD-09-CM (par. 5.3.3. disc. tecn.), nonché di espungere dallo schema la rilevazione di comportamenti quali il "gioco d'azzardo patologico" e l'uso di "tecnologie digitali" che appaiono, con evidenza, eccedenti rispetto alle finalità del decreto il cui ambito di applicazione è la sola dipendenza da sostanze stupefacenti o da alcool anche in conformità a quanto previsto dalla normativa di settore (par. 5.3.5. "Codice sostanza, uso o comportamento" nn. 23 e 24, disc. tecn.; art. 2, comma 1, lett. c), d.P.R. n. 309/1990; art. 1 dello schema).

5.4. Nell'individuare i soggetti dai quali le aziende sanitarie locali ricevono informazioni relative agli assistiti, il disciplinare tecnico fa riferimento anche all'autorità giudiziaria relativamente a casi di adozione di provvedimenti giudiziari a carico degli interessati (par. 5.3.4. "Tipologia invio" n. 4); artt. 90 e 94 d.P.R. n. 309/1990). Poiché tali informazioni possono costituire "dati giudiziari" ai sensi del Codice in materia di protezione dei dati personali (art. 4, comma 1, lett. e), del Codice), si

richiama l'attenzione sulla circostanza che, allo stato, il ministero, le regioni e le province autonome non possono trattare tali dati per le finalità del presente decreto in quanto il loro trattamento non è previsto dai citati regolamenti sui dati sensibili e giudiziari per finalità di programmazione dell'assistenza sanitaria.

6. L'utilizzo del sistema e la sicurezza dei dati

La particolare delicatezza dei dati trattati nell'ambito del SIND ne impone, come abbiamo già detto, un utilizzo proporzionato rispetto alle finalità perseguite e rende, altresì, necessaria una particolare attenzione alla sicurezza del sistema informatico utilizzato e, sul piano applicativo, all'integrità dei dati trasmessi, mediante l'adozione di misure di sicurezza calibrate rispetto alle modalità di raccolta dei dati, conformi agli articoli 22, 31 e ss. e all'Allegato B del Codice.

In tal senso, è necessario integrare lo schema di decreto:

- a) perfezionando la disposizione che prevede il ricorso a tecniche di cifratura dei dati sensibili (art. 5, comma 4) come segue: “I dati inviati dalle regioni e province autonome, già privi degli elementi identificativi diretti, sono archiviati previa separazione dei dati sanitari dagli altri dati. I dati sanitari sono trattati con tecniche crittografiche.”;
- b) accrescendo la sicurezza dell'accesso al front-end web dell'applicazione (predisposto per l'accesso al di fuori del Sistema pubblico di connettività) mediante l'adozione di un protocollo sicuro https con autenticazione bilaterale (mutual authentication) basata su certificati digitali emessi da una autorità di certificazione ufficiale;
- c) prevedendo nel disciplinare tecnico di adottare adeguate misure per la distruzione sicura dei supporti di memorizzazione dei dati sensibili, eventualmente indicandole (allegato B del Codice, regola 22; par. 3.2.1. disc. tecn.);
- d) prevedendo il tracciamento delle operazioni di accesso al sistema dedicato alla memorizzazione dei dati (data server), specie quelle che eventualmente possano avvenire al di fuori del contesto applicativo, cioè di tutte quelle operazioni che possano avvenire mediante accesso diretto al data base e per il rilevamento di eventuali anomalie (par. 3.2 “Caratteristiche infrastrutturali”);
- e) in riferimento alle misure di registrazione, autenticazione e accesso degli utenti e alla parola chiave, integrando lo schema con riferimento a tutte le indicazioni contenute nella regola 5 dell'Allegato B del Codice, e in particolare a quelle che consigliano l'utilizzo di una parola chiave di almeno otto caratteri, se possibile, che non contenga riferimenti agevolmente riconducibili all'incaricato (par. 3.3 “Abilitazione degli utenti”).

Il Garante richiama infine l'attenzione, sul piano formale, sulla necessità di prevedere nel preambolo il parere del Garante e di precisare se, come sembra, i flussi di dati previsti dal presente decreto siano destinati a sostituire quelli di cui al d.m. 20 settembre 1997 citato nel medesimo preambolo.

ciò premesso il garante:

esprime parere favorevole sullo schema di decreto recante l'istituzione del sistema informativo per le dipendenze (SIND) a condizione che, nei termini di cui in premessa:

- a) siano indicate espressamente e in maniera esaustiva nell'articolato del decreto le finalità per le quali i dati sono raccolti nel SIND e che si intendono perseguire mediante il sistema (punto 1);
- b) le parole “informazioni individuali ma non nominative”, ovunque ricorrano, siano sostituite con quelle, più corrette, di “dati personali non identificativi” (punto 2);
- c) sia previsto che le regioni e le province autonome che non dispongono di sistemi di codifica utilizzino solo dati anonimi (punto 2);
- d) siano individuate specificamente, nell'articolato, le unità organizzative del ministero, delle regioni e delle province cui è consentito il trattamento delle informazioni e i limiti entro i quali possono accedere ai dati raccolti mediante il SIND (punto 3);

- e) siano assicurati, mediante disposizioni ad hoc, l'accesso selettivo ai dati e la rappresentazione aggregata delle informazioni (punto 3);
- f) siano specificati nel disciplinare tecnico i dati che devono essere comunicati nel caso di richiesta di anonimato da parte di un soggetto tossicodipendente (punto 4);
- g) siano effettuate le valutazioni richieste e siano adottate le modifiche al decreto in chiave di proporzionalità specificamente indicate al punto 5;
- h) sia integrato lo schema con mirate disposizioni in materia di misure di sicurezza nel trattamento dei dati (punto 6).

Roma, 6 maggio 2009

Il Presidente, Pizzetti

Il Relatore, Fortunato

Il Segretario Generale, Patroni Griffi