D.g.r. 28 febbraio 2013 - n. IX/4928
Sistema informativo socio-sanitario (SISS): aggiornamento d.g.r. VIII/5198 2 agosto 2007 in relazione all'individuazione dei responsabili dei trattamenti dei dati personali e alle relative istruzioni e modalità di trattamento

LA GIUNTA REGIONALE

Vista la legge regionale 30 dicembre 2009, N. 33 «Testo Unico delle Leggi regionali in materia di sanità»;

Vista la d.g.r. VIII/10031 del 7 agosto 2009 «Determinazioni in merito all'evoluzione del Progetto CRS-SISS»;

Vista la d.g.r. VIII/10512 del 9 novembre 2009 «Determinazioni in merito all'evoluzione del Progetto CRS-SISS – Approvazione della pianificazione di dettaglio, dello schema d'incarico a Lombardia Informatica s.p.a. e degli schemi di convenzione tra Regione Lombardia, Lombardia Informatica s.p.a. e Aziende Sanitarie»;

Vista la Convenzione Quadro tra la Giunta regionale della Lombardia e Lombardia Informatica s.p.a. del 7 marzo 2011, inserita al n. 14944/RCC della Raccolta Convenzioni e Contratti di Regione Lombardia;

Considerato che Regione Lombardia per la realizzazione del SISS ha predisposto, avvalendosi di Lombardia Informatica s.p.a., una piattaforma tecnologica infrastrutturale che viene messa a disposizione di Regione Lombardia stessa e delle Aziende Socio-Sanitarie pubbliche e private accreditate a contratto, per la comunicazione ed elaborazione dei dati sanitari amministrativi e clinici;

Visto il d. lgs. 30 giugno 2003, n. 196 «Codice in materia di protezione dei dati personali», in particolare gli artt. 4 (definizioni), 20 e 21 (principi applicabili al trattamento di dati sensibili), 33-36 (misure minime di sicurezza);

Visto il regolamento regionale 24 dicembre 2012 n. 3 «Regolamento per il trattamento dei dati sensibili e giudiziari di competenza della Giunta regionale, delle aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione Lombardia (artt. 20-21 del d. lgs. 196/2003)», in cui vengono disciplinati i trattamenti che effettuano, come Titolari, la Regione Lombardia e le Aziende Sanitarie;

Considerato il d.l. 18 ottobre 2012, n. 179 «Ulteriori misure urgenti per la crescita del Paese», convertito con modificazione dalla legge n. 221 del 17 dicembre 2012, con particolare riferimento alla Sezione IV Sanità Digitale;

Considerati i mutamenti intervenuti in termini di nuovi assetti societari del gruppo Lombardia Informatica e l'emissione –da parte della Regione Lombardia– di specifici documenti che disciplinano e semplificano il processo di designazione a Responsabili del trattamento di dati personali;

Considerate le aggiudicazioni delle Gare d'Appalto bandite da Lombardia Informatica s.p.a. per il prosieguo delle attività relative al SISS (*Gara 5/2012/LI - Procedura aperta ai sensi del d.lgs. n. 163/2006 per l'affidamento dei servizi di sviluppo e manutenzione, assistenza, supporto all'analisi dei processi/demand management e territorio per la realizzazione dei modelli di e-health della Regione Lombardia. Cod. SISS 1, Gara 6/2012/LI - Procedura aperta ai sensi del d.lgs. n. 163/2006 per l'affidamento dei servizi di sviluppo e manutenzione, assistenza, supporto all'analisi dei processi/demand management, territorio e formazione per la realizzazione dei modelli di e-health della Regione Lombardia. Cod. SISS 2 e Gara 7/2012/LI - Procedura aperta ai sensi del d.lgs. n. 163/2006 per l'affidamento dei servizi di sviluppo e manutenzione, assistenza, supporto all'analisi dei processi/demand management e formazione per la realizzazione dei modelli di e-Government della Regione Lombardia. Cod. TRASVERS*), che hanno portato all'individuazione dei nuovi Fornitori;

Ritenuto necessario provvedere all'aggiornamento dei soggetti individuati come Responsabili del trattamento dei dati e provvedere all'aggiornamento delle istruzioni e modalità di trattamento precedentemente definite con la d.g.r. VIII/5198 del 2 agosto 2007 «Progetto Carta Regionale dei Servizi - Sistema Informativo Socio-Sanitario (CRS-SISS): individuazione dei Responsabili dei trattamenti dei dati personali – Disposizioni per le Aziende Sanitarie pubbliche e schema di convenzione con le Aziende Socio-Sanitarie private accreditate a contratto»;

Ritenuto necessario provvedere, a seguito dei nuovi assetti societari del Gruppo Lombardia Informatica ad individuare quali Responsabili dei trattamenti dei dati personali nell'ambito del SISS, ognuno per le rispettive competenze, Lombardia Informatica s.p.a. e Lombardia Gestione s.p.a. disciplinando i ruoli, i compiti e le responsabilità di tali soggetti secondo le indicazioni di cui all'Allegato 1, «Modalità di trattamento dei dati personali effettuato dai soggetti individuati come Responsabili del trattamento nell'ambito del SISS», parte integrante del presente provvedimento;

Ritenuto inoltre necessario provvedere ad individuare quali Responsabili dei trattamenti dei dati personali nell'ambito del SISS, ognuno per le rispettive competenze, i Fornitori individuati a seguito dell'aggiudicazione delle Gare d'Appalto bandite da Lombardia Informatica s.p.a. per il prosieguo delle attività relative al SISS ovvero, Almaviva s.p.a., Bit Media s.p.a., Santer Reply s.p.a., Telecom Italia s.p.a., Lutech s.p.a., Capgemini Italia s.p.a. e Sopra Group s.p.a., disciplinando i ruoli, i compiti e le responsabilità di tali soggetti secondo le indicazioni di cui all'Allegato 1, «Modalità di trattamento dei dati personali effettuato dai soggetti individuati come Responsabili del trattamento nell'ambito del SISS», parte integrante del presente provvedimento;

Considerato che le società Telecom Italia s.p.a., Lutech s.p.a. e Almaviva s.p.a. e i loro sub-fornitori, designati Responsabili del trattamento di dati personali ai sensi della d.g.r. VIII/5198 del 2 agosto 2007, hanno cessato i trattamenti a loro precedentemente affidati a seguito della d.g.r. stessa;

Ritenuto, a seguito della cessazione delle attività di cui sopra, di dover dar seguito a quanto previsto dall'art. 16 del d.lgs. 196/2003 in relazione alla cessazione dei trattamenti da parte delle società Telecom Italia s.p.a., Lutech s.p.a., Almaviva s.p.a. e dei loro sub-fornitori;

A voti unanimi espressi nelle forme di legge;

DELIBERA

1. di aggiornare la d.g.r. VIII/5198 del 2 agosto 2007 con l'individuazione dei soggetti Responsabili dei trattamenti *ex* d.lgs. 196/2003 e con la conseguente definizione delle istruzioni e modalità di trattamento;

2. di designare Responsabili dei trattamenti di dati personali di cui la Regione è Titolare per finalità istituzionali, nell'ambito del SISS, ognuna per le proprie competenze, le società: Lombardia Informatica s.p.a., Lombardia Gestione s.p.a., e i Fornitori individuati nelle Gare, ovvero Almaviva s.p.a., Bit Media s.p.a., Santer Reply s.p.a., Telecom Italia s.p.a., Lutech s.p.a., Capgemini Italia s.p.a. e Sopra Group s.p.a. disciplinando i ruoli, i compiti e le responsabilità di tali soggetti secondo le indicazioni di cui all'Allegato 1 «Modalità di trattamento dei dati personali effettuato dai soggetti individuati come Responsabili del trattamento nell'ambito del SISS», parte integrante del presente provvedimento;

3. di demandare alle Direzioni regionali competenti la comunicazione, alle società Telecom Italia s.p.a., Lutech s.p.a., Almaviva s.p.a. e ai loro sub- fornitori, designati Responsabili del trattamento di dati personali ai sensi della d.g.r. VIII/5198 del 2 agosto 2007, sia della cessazione dei trattamenti svolti in base alle attività precedentemente assegnate, sia dell'indicazione degli adempimenti conseguenti a tale cessazione secondo quanto previsto dall'art. 16 del d. lgs. 196/2003;

4. di dare atto che con l'approvazione del presente atto nulla innova rispetto a quanto definito negli Allegati alla d.g.r. VIII/5198 del 2 agosto 2007, con particolare riferimento ai Requisiti Minimi di Sicurezza per gli Aderenti al SISS, alle Disposizioni regionali alle Aziende Sanitarie Pubbliche e agli IRCCS di diritto pubblico e allo Schema di convenzione con i Soggetti Privati Accreditati a contratto;

5. di provvedere alla pubblicazione del presente provvedimento sul BURL e sui siti delle Direzioni Generali Sanità e Famiglia, Conciliazione, Integrazione e Solidarietà Sociale e di inviare copia del provvedimento all'Autorità Garante per la Protezione dei dati personali.

Il segretario: Marco Pilloni

——— • ———

ALLEGATO 1

"MODALITÀ DI TRATTAMENTO DEI DATI PERSONALI EFFETTUATO DAI SOGGETTI INDIVIDUATI COME RESPONSABILI DEL TRATTAMENTO NELL'AMBITO DEL SISS"

ISTRUZIONI AI RESPONSABILI DEL TRATTAMENTO

I Responsabili dei trattamenti individuati sono tenuti ad effettuare i trattamenti dei dati nel rispetto di quanto disposto dal Codice in materia di Protezione dei dati personali, D. Lgs. n. 196/2003 e s.m.i. e di ogni ulteriore provvedimento del Garante per la Protezione dei dati personali, secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli Interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

I Responsabili sono tenuti a trattare i dati personali nel rispetto dei principi di necessità, pertinenza e non eccedenza, in modo lecito e secondo correttezza, per scopi legittimi e determinati, assicurando l'esattezza e la completezza dei dati e conservando i dati in una forma che consenta l'identificazione dell'Interessato per un periodo non superiore a quello occorrente alle finalità per i quali sono stati raccolti e trattati, e provvedendo, quando necessario, alla loro rettifica e aggiornamento.

I Responsabili sono tenuti ad iniziare eventuali nuovi trattamenti solo in seguito a richiesta da parte di Regione Lombardia, Titolare del trattamento.
In caso di revoca della designazione a Responsabili dei trattamenti, o di cessazione di un trattamento, i Responsabili dovranno seguire le istruzioni impartite dal Titolare ed in assenza di queste provvedere alla distruzione dei dati personali inerenti il SISS in suo possesso, ai sensi dell'artico 16 comma 1 lettera a del D. Lgs. n. 196/2003.

I Responsabili sono tenuti ad adottare, in relazione al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, tutte le misure di sicurezza idonee a evitare rischi di distruzione, danneggiamento o perdita, anche accidentale, dei dati, nonché pericoli di accesso non autorizzato o di trattamento non consentito o non conforme alla alle finalità della raccolta, secondo quanto previsto dal D. Lgs. n. 196/2003 s.m.i.. In particolare, devono assicurare in ogni momento che la sicurezza fisica e logica dei dati oggetto di trattamento sia conforme alle norme vigenti, ai documenti contrattuali e di specifiche dei Servizi definiti da Regione Lombardia avvalendosi di Lombardia Informatica S.p.A., nonché alle disposizioni contenute nel Documento Programmatico per la Sicurezza[1] prodotto dalla Regione Lombardia per il SISS. Le misure di sicurezza adottate dovranno in ogni situazione uniformarsi allo "standard" di maggiore sicurezza fra le disposizioni di legge e gli elementi contrattuali e/o progettuali.

I Responsabili**,** ciascuno per i trattamenti assegnati**,** sono inoltre tenuti a:

1. individuare per iscritto gli Incaricati del trattamento dei dati personali (persone fisiche o gruppi omogenei), impartire loro le istruzioni idonee alle attività da svolgere e vigilare sul loro operato;

2. elaborare un piano di formazione destinato agli Incaricati;

3. assicurarsi che ad ogni Incaricato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'Incaricato, eventualmente associato a un codice identificativo o a una parola chiave;

4. prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso ed uso esclusivo dell'Incaricato;

5. assicurare che la parola chiave, quando è prevista dal sistema di autenticazione, sia composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato e deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi;

6. assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri Incaricati, neppure in tempi diversi;

7. assicurare che sia operata la cancellazione del codice identificativo personale in caso venga a cessare la necessità di accesso da parte dell'Incaricato o intervenga un'inattività per più di sei mesi;

8. predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici.
   In tal caso la custodia delle copie delle credenziali deve essere organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia;

9. prevedere, con criteri restrittivi, profili di autorizzazione di accesso per ogni singolo Incaricato o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti;

10. prevedere l'impiego di sistemi di autorizzazione che, secondo il concetto che "è vietato ciò che non è espressamente permesso", consentono di accedere ai dati per effettuare le operazioni di trattamento secondo il proprio specifico profilo utente;

1 Regione Lombardia ha deciso di continuare a redigere ed aggiornare annualmente il DPS, nonostante la recente abrogazione dell'obbligo normativo.

11. verificare, ad intervalli almeno annuali, la sussistenza delle ragioni che hanno portato al rilascio della autorizzazione;

12. assicurare che nel caso di Operatori telefonici, Incaricati del trattamento, questi nelle comunicazioni vocali scambiate durante lo svolgimento delle proprie attività si conformino alle disposizioni specificatamente emesse dai Responsabili del trattamento per il rispetto dell'Utenza e la riservatezza delle informazioni trattate;

13. redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del Titolare e implementare le ulteriori misure, come definito nel Provvedimento dell'Autorità Garante per la Protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" e s.m.i.;

14. installare sugli elaboratori idonei programmi contro il rischio di intrusione e accesso abusivo in accordo ai requisiti di legge da aggiornare comunque ogni sei mesi ed in occasione di ogni versione disponibile dalla casa costruttrice;

15. prevedere, ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, all'aggiornamento, entro un periodo di tempo non superiore a sei mesi, dei programmi utilizzati, o almeno alla valutazione degli impatti sull'aggiornamento;

16. prevedere l'adozione di copie di back-up e il ripristino dei dati in tempi certi e comunque non superiori a sette giorni.

Inoltre per il trattamento di dati sensibili, cioè quelli di cui al art. 4 comma d) del D. Lgs. 196/2003, i Responsabili devono:

1) prevedere che il riutilizzo dei supporti di memorizzazione sia possibile solamente nel caso in cui le informazioni precedentemente contenute non siano recuperabili; in caso contrario i supporti dovranno essere distrutti. In questo ambito risulta necessario procedere a:
   a) emanare adeguate istruzioni di comportamento a tutti gli Incaricati;
   b) effettuare una ricognizione completa di tutti i supporti di memoria che possano essere riutilizzabili, sia essi di tipo asportabile che presenti in aree di memoria interne al sistema operativo od in programmi, ove possano trovarsi dati sensibili;
   c) esaminare tutti i nuovi supporti, sistema operativo e programmi, che vengono inseriti nel sistema di trattamento dei dati, analizzando i possibili rischi ed impartendo specifiche istruzioni agli Incaricati.

2) assicurare che la memorizzazione dei dati sensibili su elenchi, registri o banche dati, avvenga in maniera da non permettere la diretta identificazione dell'interessato, ovvero che la memorizzazione dei dati sensibili sia cifrata o in alternativa che vi sia separazione tra i dati sensibili e gli altri dati personali che possano permettere l'identificazione dell'interessato;

3) assicurare che il trasferimento dei dati sensibili in formato elettronico, avvenga attraverso "canali sicuri" o in maniera cifrata.

I Responsabili devono procedere ad un controllo periodico sui rischi effettivi e sulla efficacia delle contromisure adottate, e devono redigere un documento (al quale il DPS della Regione Lombardia, Titolare del trattamento, farà riferimento) che descriva le misure di sicurezza effettivamente adottate a fronte dei trattamenti assegnati ed ai requisiti sopra esposti.

In merito al **trattamento dei dati personali con strumenti diversi da quelli elettronici**, i Responsabili sono tenuti a predisporre un archivio per gli atti e i documenti con dati personali individuando per iscritto gli Incaricati con i relativi profili di accesso ai dati ed ai documenti.
Devono essere definite le procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio un registro e degli armadi separati e chiusi).
Il trattamento di dati sensibili, dovrà infine prevedere l'utilizzo di appositi contenitori con lucchetti o serrature e definire una procedura di gestione delle chiavi.

E' fatto comunque assoluto **divieto** ai Responsabili designati della **diffusione** dei dati, della **comunicazione** non autorizzata a terzi e più in generale è fatto **divieto** di effettuare trattamenti non finalizzati all'esecuzione delle attività affidate.

Le operazioni di trattamento devono essere gestite dalle singole società individuate quali Responsabili dei trattamenti ai sensi dell'art. 29, D. Lgs. n. 196/2003 in aderenza alle attività svolte nell'ambito degli specifici sottoprogetti assegnati.

Nel caso in cui i Responsabili, nel trattamento dei dati, si avvalgano di sub-fornitori, sono tenuti a comunicare tempestivamente i riferimenti degli stessi al Titolare del trattamento, che provvederà a designarli individualmente come Responsabili, dettando compiti e istruzioni.

I Responsabili sono chiamati ad evadere tempestivamente le richieste del Titolare e degli Interessati e a proporre e/o adottare tempestivamente -se del caso d'intesa con altri soggetti Responsabili- nel rispetto delle indicazioni espresse dal Titolare, ogni soluzione organizzativa, logistica, tecnica e procedurale idonea ad assicurare l'osservanza delle disposizioni vigenti in materia di trattamento dei dati personali in modo da consentire l'esercizio dei diritti da parte degli Interessati.

Regione Lombardia, Titolare del trattamento, come previsto dall'art. 29 c. 5 del D. Lgs. 196/2003 vigilerà sulla puntale osservanza delle istruzioni impartite ai Responsabili, effettuando periodiche azioni di verifica.