Società Italiana
Telemedicina @ Sanità Elettronica

DL SEMPLIFICAZIONI E SOPPRESSIONE DEL DPS: I SUGGERIMENTI DELLA SIT

Sul supplemento ordinario alla G.U. n.33 del 9 febbraio 2012 è stato pubblicato il d.l. 9 febbraio 2012 n.5 "Disposizioni urgenti in materia di semplificazione e di sviluppo" che all'art. 45 "Semplificazioni in materia di dati personali", recita: "Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni: (omissis...) lettera c) **all'articolo 34 è soppressa la lettera g) del comma 1 ed è abrogato il comma 1-bis**; d) **nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B sono soppressi i paragrafi da 19 a 19.8 e 26**.

In forza del decreto in oggetto, in vigore dal 10 febbraio scorso, **non vi è più obbligo della "tenuta di un aggiornato documento programmatico sulla sicurezza", né di autocertificazione sostituiva dello stesso.**

Per quanto riguarda invece il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B al Codice, **non vi è più obbligo di presentare "entro il 31 marzo di ogni anno, un documento programmatico sulla sicurezza"**, né sono più definite le caratteristiche che tale documento avrebbe dovuto avere.

Di conseguenza è soppresso anche l'obbligo di dichiarare, nella relazione accompagnatoria al bilancio, l'avvenuta redazione o aggiornamento del DPS.

Fin qui le modifiche al Codice privacy, riguardanti il DPS, introdotte dal d.l. Semplificazioni che, se da un lato ne sancisce la sua soppressione, dall'altro, occorre sottolineare con forza che **permane in vigore l'obbligo dell'adozione delle misure di sicurezza.**

Insomma ciò che conta - ai fini della legge - è l'adozione sostanziale delle misure di sicurezza, al di là di qualsiasi documentazione formale.

In pratica, pur non essendo più obbligatoria la tenuta di un aggiornato DPS, la Società italiana di telemedicina e sanità elettronica ritiene però opportuno suggerire ai medici titolari di trattamento di continuare a tenere traccia, in modo organico e coordinato, delle misure di sicurezza effettivamente adottate nello studio medico per evitare omissioni o dimenticanze che poi si potrebbero tradurre in penalità.

La tenuta di un documento del genere facilita infatti eventuali verifiche da parte delle autorità preposte e riduce la probabilità di incorrere in sanzioni.

A parere della scrivente Società scientifica, anche se la tenuta di un aggiornato DPS non è dunque più un obbligo, la redazione di un documento di analogo contenuto è pertanto una scelta vivamente consigliata!

IL COMUNICATO STAMPA DEL GARANTE PRIVACY

DECRETO LEGGE 9 FEBBRAIO 2012, N. 5: SOPPRESSIONE DEL DPS

In riferimento all'obbligo, finora previsto, dell'aggiornamento entro il 31 marzo di ogni anno del **Documento Programmatico per la Sicurezza (DPS)**, si segnala che il **d.l. 9 febbraio 2012, n. 5** - attualmente all'esame del Parlamento per la conversione in legge - ha, tra l'altro, modificato alcune disposizione del Codice in materia di protezione di dati personali, sopprimendo in particolare dagli adempimenti in materia di misure minime di sicurezza proprio il Documento Programmatico per la Sicurezza.

Pertanto, salvo che intervengano modifiche da parte del Parlamento, l'obbligo di redigere e aggiornare periodicamente il citato DPS è venuto meno.

VADEMECUM PER I MEDICI DI MEDICINA GENERALE

Innanzitutto occorre ricordare che prima di effettuare qualsiasi tipo di trattamento dati è necessario acquisire il consenso validamente espresso per iscritto (dati sensibili) dell'interessato (il paziente), dopo avergli fornito idonea informativa inerente finalità e modalità di trattamento, comprese le misure di sicurezza adottate, i soggetti a cui possono essere comunicati i dati, o che possono venirne a conoscenza in qualità di responsabili o incaricati di trattamento, l'ambito di diffusione ed i diritti dell'interessato. I dati possono essere trattati anche senza consenso per la salvaguardia della vita dell'interessato, o per l'incolumità fisica di un terzo, oppure quando è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria.

Nella pratica dello studio del medico di medicina generale, ma anche del pediatra di libera scelta, i soggetti che possono avere accesso ai dati degli assistiti sono:

- il medico titolare;
- i sostituti ed i colleghi associati della medicina di gruppo o di rete;
- gli addetti alla segreteria ed il personale infermieristico;
- i tecnici informatici;
- le società che eseguono la manutenzione su apparati diagnostici informatizzati (ecografi, spirometri, elettrocardiografi ecc…) che consentano anche una minima archiviazione dei dati dei pazienti.

Tutte queste figure, per via degli obblighi previgenti, devono avere ricevuto le loro istruzioni operative, si deve aver provveduto alla profilazione degli utenti in base al ruolo svolto, con apposite scelte circa le autenticazioni (chi accede) e autorizzazioni (cosa può vedere e/o modificare) in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

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, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

La parola chiave, quando è prevista dal sistema di autenticazione, è 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 contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici 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. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

I dati personali sono protetti contro il rischio di intrusione (trojan) e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale (malware), mediante l'attivazione di idonei strumenti elettronici (antivirus, firewall) da aggiornare con cadenza almeno semestrale (consigliata: settimanale o, in automatico, appena disponibile).

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (sistema operativo ed applicativi vari) sono effettuati con cadenza almeno semestrale (consigliata: mensile o, in automatico, appena disponibile).

I dati sensibili sono protetti contro l'accesso abusivo, di cui all'art. 615-*ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici (firewall).

I dati devono essere salvati (backup) con frequenza almeno settimanale (consigliata: giornaliera).

Devono essere impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati (CD, DVD, hard-disk esterni etc.) al fine di evitare accessi non autorizzati e trattamenti non consentiti.

I supporti rimovibili (CD, DVD, hard-disk esterni etc.) contenenti dati sensibili se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Devono essere adottate idonee misure per garantire il ripristino dell'accesso ai dati (restore) in caso di danneggiamento degli stessi o degli strumenti elettronici (disaster recovery) in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni (consigliato: un giorno). Devono essere installati dispositivi elettronici atti a garantire l'alimentazione elettrica (gruppi di continuità) in caso di black-out o sbalzi di tensione (filtri di protezione) in modo tale da preservare l'integrità dei dati e degli archivi elettronici per un tempo sufficiente a consentire il loro salvataggio e la chiusura ordinata delle applicazioni e del sistema informatico.

I dati sensibili devono essere trattati in maniera disgiunta dagli altri dati personali che permettano di identificare direttamente gli interessati. I dati relativi all'identità genetica devono essere trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti. Il trasferimento dei dati in formato elettronico (trasmissione telematica di dati sanitari e sensibili) deve essere cifrato.

Nel caso di soggetti quali: tecnici informatici o softwarehouse che si occupano dell'aggiornamento e della manutenzione del sistema informatico, di ditte che fanno assistenza tecnica sugli apparati diagnostici, ci deve già essere (o si deve procedere se non si è fatta) la nomina a responsabili esterni.

I medici sostituti ed i colleghi delle forme associative complesse delle "medicine di gruppo o delle medicine in rete" sono da indicare come responsabili di trattamento, da parte del medico titolare.

Gli addetti alla segreteria ed il personale infermieristico sono nominati quali incaricati del trattamento.

Nel caso di stagisti o di utilizzo temporaneo, si utilizzano apposite "lettere di riservatezza" che vincolino l'utente.

Si ricorda infine che in base al Provvedimento del Garante del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008), la definizione di "amministratore di sistema" generalmente riferita, in ambito informatico, a figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione dati o di sue componenti, è estesa anche agli amministratori di basi di dati, agli amministratori di reti e di apparati di sicurezza e agli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

La rilevanza, la specificità e la particolare criticità del ruolo dell'amministratore di sistema sono state pertanto considerate anche dal legislatore il quale ha individuato, con diversa denominazione, particolari funzioni tecniche che, se svolte da chi commette un determinato reato, integrano ad esempio una circostanza aggravante.

Le forme associative complesse della medicina generale quali quelle delle “medicine di gruppo o delle medicine in rete”, possono prevedere pertanto delle figure riconducibili a quello che il Garante definisce come "amministratore di sistema".

Tra gli obblighi previsti per gli amministratori di sistema, si ricorda che vi è anche quello della registrazione degli accessi, devono cioè essere adottati sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo di tempo, non inferiore a sei mesi (consigliato: due anni).

CONCLUSIONI

Il DPS, non più obbligo legislativo, può mantenere la sua funzione di strumento analitico e di sintesi ad uso del titolare e del privacy manager per poter applicare e gestire al meglio le misure di sicurezza e, quindi, per mantenere la qualità, la correttezza, la disponibilità e l'obbligatoria riservatezza del dato clinico.

Dopo varie proroghe, l'obbligatorietà della redazione del DPS (che, ricordiamo, non necessitava di "data certa") risale ormai al 31 marzo 2006, cioè sono sei anni che i medici sono abituati a redigerlo: il suggerimento della SIT è quello di continuare a farlo, specie se nel frattempo, non sono intervenute variazioni. In alternativa, in luogo del DPS, si consiglia comunque la redazione di un documento analitico equivalente che tenga nota, in modo aggiornato, delle misure di sicurezza effettivamente adottate, specie se nel frattempo sono intervenute invece delle variazioni.

Si ricorda infine che, ai sensi del Codice Privacy:

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

In questi casi la prova liberatoria consiste proprio nella prova di avere adattato tutte le misure idonee ad evitare il danno.

Art. 161. Omessa o inidonea informativa all'interessato

La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro.

Art. 162. Altre fattispecie

2-bis. In caso di trattamento di dati personali effettuato in violazione delle misure indicate nell'articolo 33 o delle disposizioni indicate nell'articolo 167 è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da ventimila euro a centoventimila euro. Nei casi di cui all'articolo 33 è escluso il pagamento in misura ridotta.

2-ter. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'articolo 154, comma 1, lettere c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro.

Art. 167. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Art. 169. Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni.

APPROFONDIMENTI NORMATIVI

DECRETO-LEGGE 9 febbraio 2012, n. 5
Disposizioni urgenti in materia di semplificazione e di sviluppo.
(*G.U. n. 33 del 9-2-2012 – Supplemento Ordinario n.27)*

Art. 45 Semplificazioni in materia di dati personali.

1. Al decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni: a) all'articolo 21 dopo il comma 1 è inserito il seguente: «1-bis. Il trattamento dei dati giudiziari è altresì consentito quando è effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, che specificano la tipologia dei dati trattati e delle operazioni eseguibili.»; b) all'articolo 27, comma 1, è aggiunto, in fine, il seguente periodo: "Si applica quanto previsto dall'articolo 21, comma 1-bis."; c) all'articolo 34 è soppressa la lettera g) del comma 1 ed è abrogato il comma 1-bis; d) nel disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B sono soppressi i paragrafi da 19 a 19.8 e 26.

In forza del decreto in oggetto, in vigore dal giorno successivo alla pubblicazione in G.U. ed in attesa di eventuali modifiche introdotte dalla legge di conversione, è pertanto soppressa la lettera g) del comma 1 ed è abrogato il comma 1-bis dell'art.34 del Codice privacy, cioè **non vi è più obbligo della "tenuta di un aggiornato documento programmatico sulla sicurezza"** (art. 34, comma 1, lett. g) **né di autocertificazione sostituiva del DPS** "per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili e giudiziari quelli relativi ai propri dipendenti e collaboratori, anche se extracomunitari, compresi quelli relativi al coniuge e ai parenti" (modalità semplificate ex art.34 comma 1 bis).

Per quanto riguarda invece il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B al Codice, sono soppressi i **paragrafi 19**, **cioè l'obbligo di presentare "entro il 31 marzo di ogni anno"**, da parte del "titolare di un trattamento di dati sensibili o di dati giudiziari", anche attraverso il responsabile, se designato, **"un documento programmatico sulla sicurezza"** e le caratteristiche che tale documento avrebbe dovuto avere "contenente idonee informazioni riguardo":

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Di conseguenza è soppresso anche l'obbligo di dichiarare, nella relazione accompagnatoria al bilancio, l'avvenuta redazione o aggiornamento del DPS, previsto dall'art. 26 dell'Allegato B al Codice: "Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza".

Bologna, 20 febbraio 2012

Documento redatto a cura del Gruppo di studio "Sicurezza e Privacy" della SIT

(Coordinatrice: Chiara Rabbito. Componenti: Corrado Giustozzi, Michele Martoni, Andrea Monti, Graziano de' Petris, Filomena Polito. Uditrice: Silvia Casagrande) in collaborazione con il CIRSFID (Direttore: Carla Faralli) - Università di Bologna "Alma Mater Studiorum".

