Il documento programmatico della sicurezza

Data 12 dicembre 2005
Autore admin

Entro il 31 dicembre 2005 tutti gli studi medici ed i professionisti che trattano dati personali, sensibili o giudiziari, sia in forma cartacea che informatizzata devono redigere il Documento Programmatico sulla Sicurezza (DPS o DPSS) ed adeguarsi alle norme minime di sicurezza. Si tratta di un'autocertificazione che deve riportare un'analisi dettagliata di tutte le misure minime di sicurezza, così come regolamentato nei vari articoli ed Allegati del D.L. 196/2003 e nei successivi chiarimenti, che il titolare del trattamento, in base ad un'analisi dei rischi, ha messo o metterà in atto per garantire la riservatezza e sicurezza dei propri dati. Nella pratica, il legislatore chiede al medico di effettuare un' analisi/riflessione sulle metodiche con cui sono conservati i dati, sui trattamenti cui sono sottoposti e sull'assetto informatico nel suo insieme.

Il Titolare dei dati (figura espressamente prevista dal testo legislativo),quindi, procede a questa auto analisi con l'obiettivo di individuare e descrivere in particolare i seguenti punti espressamente indicati dal Garante della Privacy :-
Analisi ed individuazione dei trattamenti operati; descrizione sintetica, natura dei dati, struttura di riferimento ed eventuali altre strutture esterne che hanno accesso ai dati
- Elenco dei trattamenti con descrizione degli strumenti informatici utilizzati; individuazione delle banche dati, descrizione del supporto su cui risiedono, individuazione della tipologia dei dispositivi di accesso e tipologia di interconnessione
- Analisi delle strutture preposte al trattamento dei dati; individuazione delle stesse e del responsabile, elencazione dei trattamenti operati per ogni struttura e descrizione sintetica dei compiti della struttura
- Analisi rischi legati al comportamento del personale; definizione del livello di gravità stimata (rischi principali presi in considerazione: furto di credenziali, carenza di consapevolezza, comportamenti sleali, errori materiali, etc)
- Analisi rischi legati agli strumenti; definizione del livello di gravità stimata (azione virus o codici malefici, spamming o altre tecniche di sabotaggio, malfunzionamento o degrado degli strumenti, accessi non autorizzati, intrusioni informatiche, intercettazioni dati trasmessi via rete, etc)
- Analisi rischi dovuti ad eventi legati al contesto; definizione del livello di gravità stimata (accessi non autorizzati ai locali, furto di strumenti, eventi distruttivi dolosi o accidentali, guasto a sistemi complementari, errori umani nella gestione della sicurezza, etc)
- Elenco delle misure di sicurezza adottate o da adottare; descrizione con definizione dei trattamenti dati interessati ed indicazione delle misure di sicurezza già adottate o da adottare (i principali: formazione dipendenti, antivirus, controlli su pc, controlli locali e strutture, firewall, protezione e-mail e rubriche telefoniche, impianti e verifiche installazioni, cambio password, controlli sul server centrale, analisi sistemi raid, analisi sistemi ups, protezione trasmissioni dati tra varie sedi)

- Descrizione dettagliata delle misure adottate per ogni identificativo di rischio; descrizione della misura ed identificazione del responsabile applicazione e controlli sul rischio (queste descrizioni descrivono dettagliatamente le misure adottate e la loro adeguatezza in rapporto alle misure minime definite nell'allegato B del Dlgs. 196/2003)
- Analisi sui criteri e sulle modalità di salvataggio e di ripristino dei dati; indicazione per ogni banca dati degli strumenti usati, della procedura utilizzata, della frequenza del backup, della ubicazione di conservazione delle copie, degli incaricati al backup e delle procedure di ripristino–test
- Analisi soggetti esterni che effettuano trattamenti dati; individuazione della attività esternalizzata, del tipo di dati interessati, del soggetto e descrizione dei criteri adottati per l'adozione delle misure di legge
Il Medico dovrebbe obbligatoriamente dotarsi di efficaci sistemi di sicurezza (personal firewall, antivirus aggiornati, strumenti di crittografia, lettori biometrici per la lettura delle impronte digitali, nel caso di archivi actacei armadi blindati o similari!) per l'accesso protetto ai dati presenti sul suo personal computer o ai documenti dell'archivio cartaceo.
Una volta redatto il Documento Programmatico sulla Sicurezza, il Medico deve individuare tutte le persone che hanno accesso ai dati ed a ciascuna deve dire esattamente come si deve comportare. Inoltre, deve predisporre le informative da dare a tutti coloro che gli affidano dati in cui spiega le metodiche usate nei trattamenti; tutto questo per poter completare adeguatamente il lavoro di autocertificazione.
Il DPS non deve essere spedito ma conservato.
Questo provvedimento è del tutto estraneo alla realtà. Ha una visione del lavoro dei medici all'americana, con grandi strutture zeppe di tecnici ed impiegati che si ocupano di sicurezza, aggiornamenti, inserimento dei dati, etc. etc. Una visione lontanissima dalla nostra realtà nazionale in cui il medico spesso è solo, senza alcun aiuto sia informatico che come assistenza di studio. Per un misero compenso il povero medico dovrebbe porre in essere complesse e costose misure e procedure di protezione, assolutamente spropositate ed inapplicabili nella realtà. Dunque sarà l'ennesimo, inutile adempimento che rimarrà nella maggior parte dei casi meramente sulla carta. Le solite grida manzoniane... nihil novum sub sole!