PRIVACY

Adempimenti previsti dagli artt. 33, 34, 35, 36 D. Lgs. 196/03 (Codice sulla protezione dei dati) circa le misure di sicurezza da adottare da parte di professionisti ed associazioni professionali per il trattamento dei dati personali dei propri clienti nell'ambito del contratto di prestazione dell'opera professionale.

Trattamento con l'ausilio di mezzi elettronici (art. 34 cit.)

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono state adottate le seguenti misure minime di sicurezza:

a) autenticazione informatica: il trattamento è consentito agli incaricati dotati di credenziali di autenticazione (password, chiave informatica, altre forme di legittimazione). Tale adempimento è necessario anche in caso di professionista singolo e anche se l'elaboratore non è collegato a reti estena o interna.

b) adozione di procedure di gestione delle credenziali di autenticazione: le credenziali di autenticazione devono essere assegnate e conosciute dal solo incaricato del trattamento, le modalità di assegnazione devono consentire che le stesse credenziali non possano essere assegnate a più persone, la modificazione delle stesse ogni sei mesi (ovvero tre mesi in caso di trattamento di dati sensibili e/o giudiziari), la disattivazione automatica in caso di non uso o di perdita della qualità da parte dell'assegnatario; il titolare del trattamento, inoltre, deve impartire idonee istruzioni per la conservazione e l'accesso alle credenziali di autenticazione. In caso di singolo professionista l'adempimento comporta il solo adeguamento delle credenziali di autenticazione ogni sei (o tre) mesi.

c) utilizzazione di un sistema di autorizzazione: tale adempimento è necessario in caso di organizzazione complessa del lavoro nel quale sono individuati profili di autorizzazione di ambito diverso. In questo caso deve essere utilizzato un sistema che consenta l'attribuzione delle credenziali per ogni classe di incaricati anteriormente all'inizio del trattamento dei dati. Non è necessario in caso di singolo professionista.

d) almeno ogni anno il titolare è tenuto ad aggiornare la lista degli incaricati al trattamento e la lista degli addetti alla manutenzione o gestione degli strumenti elettronici. Nel caso di singolo professionista l'adempimento consiste nell'individuazione con cadenza almeno annuale del tecnico che procede alla manutenzione dei sistemi informatici o delle modalità con la quale ci si assicura il buon funzionamento dei sistemi informatici. Scadenza entro il 1 gennaio di ogni anno. Le modalità di aggiornamento della lista e delle mansioni degli incaricati e la loro formazione, nonché le modalità di gestione e manutenzione delle apparecchiature elettroniche devono essere indicate nel DPS. Il singolo professionista dovrà indicare solo queste ultime.

e) i dati personali devono essere protetti contro il rischio di danneggiamento dell'apparecchiatura elettronica o dei dati in essa contenuti anche mediante intrusione dall'esterno, predisponendo l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale, con scadenza entro il 1 gennaio e il 1 luglio di ogni anno. Tale adempimento è necessario in caso di connessione dell'elaboratore con la rete esterna o con rete interna qualora qualche altro elaboratore sia connesso con la rete e-

sterna. Gli aggiornamenti periodici dei programmi per l'elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti sono effettuati con cadenza annuale, con scadenza entro il 1 gennaio di ogni anno. In caso di trattamento di dati sensibili e/o giudiziari il termine è semestrale, con scadenza entro il 1 gennaio e il 1 luglio di ogni anno. Le modalità di aggiornamento devono essere riportare sul DPS, anche in caso di professionista singolo.

f) I dati devono essere salvati almeno con cadenza settimanale su supporti esterni all'elaboratore al fine di garantire l'esistenza di copie di sicurezza dei dati, nonché il ripristino e la disponibilità degli stessi. Le istruzioni circa le modalità di salvataggio, conservazione e ripristino devono essere impartite dal titolare con cadenza annuale, con scadenza entro il 1 gennaio di ogni anno e riportate sul DPS, anche in caso di professionista singolo.

g) Il titolare del trattamento di dati sensibili e/o giudiziari deve redigere, anche attraverso un responsabile (se designato), un documento programmatico sulla sicurezza (DPS) che contenga idonee informazioni circa le modalità di trattamento e il livello di misure di sicurezza adottate, con scadenza entro il 31 marzo di ogni anno. Per una migliore comprensione del DPS si rimanda in allegato sub A.

h) gli esercenti le professioni sanitarie devono effettuare il trattamento dei dati idonei a rivelare lo stato di salute o la vita sessuale, contenuti in elenchi, registri o banche dati tenuti con l'ausilio di mezzi elettronici, utilizzando tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

Trattamento senza l'ausilio di mezzi elettronici (art. 35 cit.)

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono state adottate le seguenti misure minime di sicurezza:

A) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati: il titolare deve impartire istruzioni scritte finalizzate al controllo e alla custodia degli atti e dei documenti contenenti i dati personali, per l'intero ciclo di trattamento dei dati, aggiornando tali disposizioni con cadenza annuale e, pertanto, almeno entro il 1 gennaio di ogni anno. Tale adempimento non è necessario in caso di singolo professionista.

B) predisposizione di procedure per una idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti: tale adempimento è finalizzato ad impedire che terzi non autorizzati possano accedere agli atti e documentio contenenti dati personali. Tale adempimento non è necessario in caso di singolo professionista.

C) predisposizione di procedure per la conservazione di atti e documenti in archivi con accessi selezionati e disciplina delle modalità di accesso, anche con possibile identificazione degli incaricati. Tale adempimento è necessario anche nel caso di professionista singolo al fine di impedire l'accesso agli archivi alle persone non autorizzate.
Non è prevista l'adozione del DPS.

Principi generali

I principi generali cui attenersi per rispettare le norme imposte dal Codice possono essere così sintetizzati

a) i dati personali devono essere trattati in modo pertinente e non eccedente alle finalità della raccolta (art. 11);
b) i dati trattati devono essere sempre esatti ed aggiornati se le finalità lo richiedono (art. 11);
c) i dati devono essere conservati per il solo tempo necessario agli scopi della raccolta, superato tale termine il dato deve essere cancellato (art. 11);
d) nominare in forma scritta, qualora siano presenti nella struttura, i soggetti previsti dalla legge e segnatamente: l'incaricato, il responsabile (facoltativo), l'amministratore di sistema, il soggetto preposto alla custodia delle parole chiave (questi ultimi due solo per i soggetti che trattino i dati utilizzando sistemi informatici complessi);
e) rendere agli interessati l'informativa sulle finalità del trattamento dei dati (art. 13) e le modalità di detto trattamento. Questa informativa piò essere resa anche in forma orale, la forma scritta può essere acquisita solo per fini probatori;
f) i privati e gli enti pubblici economici devono acquisire il consenso da parte dell'interessato al trattamento, anche in forma scritta, nel caso di trattamento di dati sensibili (artt. 23, 24, 26). La prestazione del consenso non è necessaria quando i dati sono trattati per finalità pubbliche o provengono da pubblici registri, come nel caso degli Ordini relativamente ai dati dei propri iscritti.

Notificazioni

Con provvedimento n. 1 del 31 marzo 2004, il Garante ha sottratto dall'obbligo di notificazione i trattamenti effettuati da esercenti le professioni sanitarie.

L'esposizione che precede, impone onerosi obblighi per i professionisti, deve però rilevarsi, che gli adempimenti descritti devono essere calibrati in base alla natura dei dati trattati, alla mole del trattamento e, soprattutto, ai mezzi con i quali detti dati vengono trattati, nonché al numero di persone che possono venire in contatto con questi dati. Con la conseguenza che un professionista che svolge individualmente la professione di psicologo, senza collaboratori di segreteria, raccogliendo dati in formato cartaceo, avrà il solo obbligo di conservare i dati in un archivio inaccessibile a terzi, mentre gli obblighi aumenteranno con l'aumentare dell'organizzazione e dei mezzi utilizzati.