

LINEE GUIDA DELL'ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI DELLA PROVINCIA DI NUORO SUL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DLGS. 30.06.2003 n. 196 "CODICE PRIVACY"

Il **1 gennaio 2004** è entrato in vigore il **Dlgs 30.06.2003 n. 196 Codice in materia di protezione dei dati personali** con il quale il legislatore ha voluto riunire in un unico testo legislativo tutte le precedenti disposizioni in tema di protezione dei dati personali.

Con l'entrata in vigore del **Dlgs 30.06.2003 n. 196** sono abrogate tutte le precedenti norme in materia di protezione dei dati personali.

Il ***Codice della privacy*** contiene norme particolari per la professione sanitaria, peraltro già soggetta all'obbligo di segreto professionale.

In particolare il **titolo V** è interamente dedicato al **trattamento di dati personali in ambito sanitario**.

Gli esercenti le professioni sanitarie – i medici e gli odontoiatri – nell'esercizio della professione trattano dati personali e in particolare dati sensibili (dati attinenti allo stato di salute) dei pazienti che si sottopongono alle loro cure.

Infatti i continui progressi della medicina che rendono vincolante, anche dal punto di vista deontologico, nel rispetto delle regole della buona pratica clinica la puntuale redazione della cartella, contenente oltre ad ogni dato obiettivo relativo alla condizione patologica e al suo decorso, le attività diagnostiche – terapeutiche praticate, obbligano di fatto il medico e l'odontoiatra alla tenuta di un archivio.

Le cartelle cliniche di ciascun paziente, riunite in un complesso organizzato di dati personali (archivio) costituisce la **banca dati**.

Il **trattamento dei dati personali** è qualunque operazione o complesso di operazioni, effettuati con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione etc. dei dati personali.

Il medico e l'odontoiatra nell'esercizio della professione è il **titolare del trattamento** dei dati personali.

La complessità della normativa, i numerosi oneri a carico del medico o dell'odontoiatra hanno determinato l'esigenza di predisporre un documento nel quale sono riassunti in maniera schematica i concetti cardine della normativa sulla tutela dei dati personali e i principali adempimenti a carico dei sanitari che per le finalità indicate dalla legge, trattano i dati personali idonei a rivelare lo stato di salute dei pazienti.

PREMESSA

Il ***Codice della privacy*** garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il Codice della privacy, nel raccomandare che il trattamento di dati personali avvenga assicurando un elevato livello di tutela dei diritti e delle libertà fondamentali, nonché del rispetto della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto di

protezione dei dati personali, impone al titolare del trattamento l'adempimento di un serie di obblighi (già previsti anche nelle normative precedenti) e il rispetto di alcune scadenze.

Questo documento ha esclusivamente la funzione di riassumere in maniera schematica i concetti cardine della normativa sulla tutela dei dati personali e i principali adempimenti a carico dei sanitari che, per le finalità indicate dalla legge, trattano i dati personali idonei a rivelare lo stato di salute dei cittadini.

Titolare del trattamento art. 4 lett. f)

Titolare del trattamento è la persona fisica (o giuridica etc.) cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Banca dati art. 4 lett . p)

Banca dati è qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Dati sensibili art. 4 lett. d)

I dati sensibili sono – tra gli altri – i dati personali idonei a rivelare lo stato di salute e la vita sessuale dei cittadini.

I dati trattati dal medico chirurgo e dall'odontoiatra sono dati sensibili e possono essere trattati:

- 1) con il **consenso dell'interessato** e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire finalità di tutela della salute o dell'incolumità fisica dell'interessato;
- 2) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

Modalità di trattamento e requisiti dei dati: art. 11

I dati personali oggetto di trattamento sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- c) esatti e, se necessario, aggiornati;
- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Informativa art. 13

L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

- a) le finalità e le modalità del trattamento cui sono destinati i dati;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;
- c) le conseguenze di un eventuale rifiuto di rispondere;

- d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venire a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- e) i diritti di cui all'art. 7;
- f) gli estremi identificativi del titolare.

*Pur non esistendo un obbligo giuridico di fornire per iscritto agli interessati (nel caso di specie ai pazienti) l'informativa con le caratteristiche su esposte, riteniamo che ragioni di opportunità, riconducibili principalmente alla prova, **consiglino al sanitario di fornire l'informativa per iscritto.***

Consenso art. 23

Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il **consenso espresso** dell'interessato.

Il consenso è validamente prestato solo se espresso **liberamente** e specificatamente in riferimento ad un trattamento chiaramente individuato, se lo stesso è **documentato per iscritto**, e se sono state rese all'interessato **le informazioni** di cui all'art. 13.

Il consenso è manifestato in *forma scritta* quando il trattamento riguarda **dati sensibili**.

Pertanto i medici e gli odontoiatri devono acquisire dai pazienti il **consenso scritto** al trattamento dei dati sensibili (nel caso di specie dati idonei a rivelare lo stato di salute e la vita sessuale).

Cessazione del trattamento art. 16

In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:

- a) distrutti;
- b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali sono raccolti;
- c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
- d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

Misure di sicurezza art. 31 e seg.

I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da **ridurre al minimo**, mediante l'adozione di idonee e preventive misure di sicurezza, **i rischi di distruzione o perdita, anche accidentale** dei dati stessi, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta.

Nel quadro dei più generali obblighi di sicurezza di cui all'art. 31, o previsti da speciali disposizioni, che rientrano nel più generale obbligo di custodire i dati per contenere il più possibile il rischio che essi siano distrutti, dispersi o conoscibili fuori dei casi consentiti o trattati in modo illecito, i titolari del trattamento sono comunque tenuti ad adottare **le misure minime individuate** nel presente capo o ai sensi dell'art. 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Il termine per adottare le nuove “*misure minime di sicurezza*” introdotte dal Codice della privacy a salvaguardia dei dati personali contenuti negli archivi e per redigere il documento programmatico sulla sicurezza (DPS) è fissato al 31 Dicembre 2004 *

Il trattamento di dati personali con strumenti elettronici è consentito solo se sono adottate le misure minime elencate nell’art. 34 tra le quali al punto g) è da segnalare la tenuta di un aggiornato documento programmatico sulla sicurezza.

Il DPS (documento programmatico sulla sicurezza) deve contenere, in particolare, l’analisi dei rischi che incombono sugli archivi – **informatici e / o cartacei** di dati personali e le tutele da adottare per prevenire la loro distruzione, l’accesso abusivo e la dispersione ed è obbligatorio per chi raccoglie utilizza e conserva dati sensibili e giudiziari.

Sul sito del Garante www.garanteprivacy.it è stata pubblicata una guida operativa per redigere il documento programmatico sulla sicurezza (DPS) che mira a facilitare l’adempimento dell’obbligo di redazione del documento programmatico.

Tuttavia non è obbligatorio utilizzare la guida per adempiere all’obbligo anche in considerazione del fatto che la stessa tiene conto dell’estrema varietà delle realtà interessate e del contesto nel quale il titolare del trattamento opera.

Pertanto, **i medici e gli odontoiatri** per la redazione del **documento programmatico sulla sicurezza** possono utilizzare anche il modello base predisposto dalla FNOMCeO contenente idonee informazioni riguardo a:

- elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell’ambito delle strutture preposte al trattamento dei dati;
- l’analisi dei rischi che incombono sui dati;
- le misure per adottare per garantire l’integrità e la disponibilità dei dati in seguito a distruzione o danneggiamento;
- 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.

Ricordiamo che il documento programmatico sulla sicurezza (DPS) deve contenere le misure minime di sicurezza” che sono soltanto una parte degli accorgimenti obbligatori in materia di sicurezza necessarie per contenere il più possibile il rischio che essi siano distrutti, dispersi, conoscibili fuori dei casi consentiti o trattati in modo illecito e di introdurre ogni utile dispositivo di protezione legato alle nuove conoscenze tecniche.

Il DPS (documento programmatico sulla sicurezza) deve essere redatto **entro il 30 marzo di ogni anno** (termine prorogato solo per l’anno 2004 al 31 Dicembre*).

A proposito della data di redazione del documento è necessario precisare che deve trattarsi di “**data certa**”.

Relativamente alle modalità per far risultare una “data certa” si dovrà applicare la disciplina civilistica in materia di prova documentale e si potranno tenere presenti i suggerimenti formulati dal Garante in un parere del 2000: a mero titolo esemplificativo la data certa può essere dimostrata attraverso apposizione di timbro postale, apposizione di numero di protocollo etc.

Riassumendo gli obblighi a carico dei sanitari (medici e odontoiatri) sono:

- dare l' informativa ai pazienti sul trattamento dei dati personali e sensibili;
- acquisire dai pazienti il consenso al trattamento dei dati;
- adottare tutte le misure di sicurezza minime e necessarie per evitare il danneggiamento o la distruzione dei dati;
- redigere entro il 30.03.2004 di ciascun anno il **Documento programmatico sulla sicurezza (DPS)**.
- Il termine per l'anno 2004 è **prorogato al 31.12.2004**, termine che deve risultare da data certa.

Ricordiamo che l' inosservanza di tali adempimenti risulta sanzionata in via amministrativa e penale.

L'art. 196 del *Codice in materia di Protezione dei dati personali* prevede l'arresto sino a due anni e/o ammenda da diecimila a cinquantamila Euro per tutti coloro che non adottano le misure minime

* **D.L. n° 266 del 09.11.2004 art. 6 proroga l'obbligo di redazione del documento programmatico al 30.06.2005 o in casi particolari al 30.09.2005**

D.Lgs. 30 giugno 2003 n. 196

ALLEGATO B

Disciplinare tecnico in materia di misure minime di sicurezza

(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. 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.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. 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 sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. 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.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-*quinquies* del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza 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, e 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, e 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.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari 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.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono 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 è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.