

D.Lgs. 196/2003
Codice in materia di protezione dei dati personali

Obblighi generali e sanzioni

per medici esercenti in regime di libera professione

Prefazione.

Il D.Lgs. n. 196/2003 *“Codice in materia di protezione dei Dati Personali”* prevede un **sistema di garanzie** a tutela dei trattamenti¹ che vengono effettuati sui dati personali.

Gli **obblighi generali prescritti** per ottemperare a tale sistema da parte dei **medici** e degli **esercenti le professioni sanitarie in regime di libera professione** sono riportati nel seguente documento ad uso esclusivo degli **affiliati dell’hms – homeopathic medicine software**. Un breve sunto delle sanzioni prescritte per le loro violazioni chiude il documento.

Introduzione.

Il medico, o qualunque altro professionista che tratti dati relativi alla salute, in qualità di Titolare² del trattamento di tali dati personali di natura sensibile, deve **ottemperare a tutte le regole e a tutti gli obblighi ed adempimenti** in materia di protezione dei dati personali **che ai sensi del D.Lgs. n. 196/2003 occorrono** per il corretto svolgimento di tali trattamenti. **L’adeguamento non consiste nella sola redazione di un Documento Programmatico sulla Sicurezza – DPS.**

In termini pratici, tali professionisti devono provvedere agli obblighi di carattere generale, alle misure di sicurezza definiti nel Disciplinare Tecnico – Allegato B del Codice – e agli specifici adempimenti che possano derivare dal trattamento sistematico di informazione genetica.

Il presente documento, da utilizzare quale guida sommaria degli argomenti, si centra sugli obblighi a carattere generale. Un secondo documento, contenente il Disciplinare Tecnico, con dei commenti inerenti l’attività svolta dal medico, vi dà delle indicazioni per l’implementazione delle misure minime di sicurezza. Una breve postilla sulle sanzioni chiude il documento.

¹ Ai fini del Codice si intende per **“trattamento”**, qualunque operazione o complesso di operazioni, effettuati anche senza l’ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l’organizzazione, la conservazione, la consultazione, l’elaborazione, la modificazione, la selezione, l’estrazione, il raffronto, l’utilizzo, l’interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati. [art. 4 / Definizioni]

² Per Medico Titolare si deve intendere il singolo professionista che esercita autonomamente, nel contesto reale del proprio esercizio, il potere decisionale sulle finalità e sulle modalità di trattamento dei dati personali dei suoi pazienti, compreso il profilo della sicurezza relativo ai dati stessi. Titolare dei dati può però anche essere lo Studio medico nel suo complesso, che deve provvedere a nominare un Titolare delegato nella persona fisica di uno dei suoi costituenti, medico od esercente la professione sanitaria.

Obblighi a carattere generale che impattano il medico o il veterinario.

1. Raccolta e modalità di trattamento.

I **dati personali**³ richiesti al paziente **devono essere** raccolti e registrati soltanto:

- per le **finalità**⁴ strettamente connesse ai fini di prevenzione, diagnosi, cura e riabilitazione e per la gestione dei rapporti di clientela stabilitisi dal momento della richiesta delle prestazioni mediche,
- e per consentire al professionista di ottemperare agli obblighi previsti da leggi, regolamenti e dalla normativa comunitaria⁵.

La persona (segretaria o assistente) che raccoglie e tratta i **dati personali identificativi** del paziente per finalità strumentali alla gestione del rapporto di clientela, deve essere autorizzata mediante un Atto di nomina, redatto da parte del Titolare.

³ Qualunque **informazione relativa a** persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

⁴ In ottemperanza agli artt. 2 e 3 (Principi di finalità e di necessità del trattamento dei dati) e all'art. 11 (Modalità del trattamento e requisiti dei dati) e al fine di garantire la sicurezza e la riservatezza dei dati.

⁵ In particolare in materia di igiene e sanità ed in relazione ad adempimenti fiscali, verifiche di carattere amministrativo, ispezioni di organi preposti alla vigilanza in materia sanitaria, investigazioni della polizia giudiziaria ecc.

I dati devono essere **raccolti direttamente presso l'interessato** nel momento in cui questi chiede di usufruire delle prestazioni mediche e devono essere trattati sia in osservanza delle regole generali per il trattamento dei dati personali (art. 11)⁶ sia degli obblighi di sicurezza dei dati e dei sistemi (art. 31) mediante l'attuazione delle Misure minime di sicurezza⁷ previste dal Disciplinare tecnico o Allegato B del Codice.

L'**inosservanza dell'art. 11 comporta danno non patrimoniale risarcibile** come espresso dall'art. 15, il quale esplicita che chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile.

Qualora vi sia una **cessazione del trattamento** dei dati bisogna procedere come stabilito dall'art. 16, vale a dire i dati sono: distrutti o cancellati; ceduti ad altro titolare, se destinati ad un trattamento compatibile agli scopi per i quali i dati sono raccolti; conservati per fini esclusivamente personali e non destinati a comunicazione sistematica o diffusione; conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici in conformità alle norme.

I dati relativi alla salute sono **raccolti e trattati soltanto dal** professionista Titolare o da colleghi con-Titolari **o da** eventuali incaricati mediante **atto di nomina** oppure, per specifiche

⁶ Al fine di garantire la sicurezza e la riservatezza, i **dati personali identificativi e relativi alla salute** richiesti al paziente **devono essere:**

raccolti e registrati per gli scopi determinati, espliciti, legittimi e se utilizzati in altre operazioni del trattamento, impiegati in termini compatibili con tali scopi, cioè trattati, nell'ambito della normale attività del Titolare, **al solo fine** degli scopi dichiarati;

trattati in modo lecito e secondo correttezza;

esatti e, se necessario, **aggiornati;**

pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;

quando possibili resi **anonimi**, in maniera che l'interessato risulti identificabile soltanto in caso di **effettiva necessità;**

conservati per un **periodo di tempo non superiore** a quello effettivamente necessario per conseguire gli scopi del trattamento;

custoditi e controllati, per evitare che altri terzi non autorizzati possano avervi accesso.

⁷ Misure Minime di Sicurezza

Nel caso in cui il trattamento dei dati venga effettuato con l'ausilio di strumenti elettronici, le misure minime elencate nell'articolo 34 sono:

- Autenticazione informatica.
- Adozione di procedure di gestione delle credenziali di autenticazione.
- Individuazione ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici e individuazione dei periodi d'aggiornamento.
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e a determinati programmi informatici.
- Adozione di procedure per custodia di copie di sicurezza e ripristino della disponibilità dei dati e dei sistemi.
- Tenuta di un DPS – Documento Programmatico sulla Sicurezza aggiornato.
- Adozione di tecniche di cifrature o di codici identificativi per trattamenti di dati relativi alla salute effettuati in ambito sanitario.

Nel caso in cui il trattamento dei dati avvenga invece senza l'ausilio di strumenti elettronici, le misure minime elencate nell'articolo 35 sono:

- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o delle unità organizzative.
- Previsione di procedure per un'adeguata custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti.
- Previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e la disciplina delle modalità di accesso, finalizzata all'identificazione degli incaricati.

operazioni, da altri professionisti della salute (specialisti, laboratorio che riceve un referto per analisi).

2. Informativa e Consenso

Ai sensi dell'art. 13 del Codice, il professionista Titolare deve **fornire al paziente (l'interessato)** le **specifiche informazioni**⁸ relative alla richiesta di dati sulla salute e all'utilizzo che di essi verrà fatto soltanto per le finalità della prestazione medica richiesta, evidenziando trattamenti di dati personali che possano presentare rischi specifici. Tale **informativa** viene resa anche al fine di consentire al paziente di rilasciare un suo **consenso** al trattamento dei dati relativi alla sua salute, accennato nell'informativa.

Inoltre, il Titolare deve **informare il paziente** sulle conseguenze del suo eventuale rifiuto a rispondere⁹, sui soggetti ai quali i suoi dati possono essere comunicati (sostituti, colleghi che forniscono prestazioni in forma associata, rappresentanti dello Stato) e sui suoi diritti quale interessato, comunicandogli, in tal senso, che qualora intenda richiedere un controllo sul trattamento dei suoi dati, per esercitare i suoi diritti deve rivolgersi al Titolare.

Il rilascio delle informazioni contenute nell'**informativa**, unitamente alla manifestazione del relativo **consenso**, debbono avvenire **prima che il Titolare o l'incaricato inizi il trattamento** dei dati identificativi e dei dati sulla salute dell'interessato.

Ricordiamo che gli esercenti le professioni sanitarie, mediante l'Autorizzazione Generale del Garante n. 2/2004 e ai sensi dell'art. 82 del Codice, possono **trattare i dati relativi alla salute senza l'informativa e senza il consenso** del paziente/interessato **in casi di**

- emergenza e di igiene pubblica,
- di prestazione medica che possa essere pregiudicata dall'acquisizione preventiva del consenso in termini di tempestività o efficacia,
- di rischio grave, imminente ed irreparabile per la salute di terzi o dell'interessato
- e in caso di impossibilità fisica o incapacità di intendere o di volere
- o non sia possibile acquisire il consenso da chi esercita legalmente la potestà.

In tali casi si procede a fare un'informativa "*a sanatoria*".

3. Protezione dei dati sulla salute del paziente mediante tecniche idonee – art. 22

Ai sensi dell'art. 22, comma 6, i dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con **tecniche di cifratura** o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

Ciò significa che tali dati sono conservati separatamente da altri dati personali, trattati per finalità che non richiedono il loro utilizzo.

⁸ Per l'informativa e - ove previsto - per il consenso si osservano, oltre alle disposizioni dell'art. 13, anche le disposizioni di cui agli articoli 23 (Consenso), 26 (Garanzie per dati sensibili) e da 75 a 82 (Settore sanitario) del Codice.

⁹ Vale a dire, l'impossibilità di concludere i termini dei rapporti.

I dati idonei a rivelare lo stato di salute non possono essere diffusi, vale a dire messi a conoscenza di soggetti indeterminati, in qualunque forma, anche mediante semplice messa a disposizione o consultazione (art. 4 / Definizioni).

4. Misure previste nell'organizzazione delle prestazioni dall'art. 83

Gli esercenti le professioni sanitarie devono adottare, **nell'organizzazione delle prestazioni** e dei servizi, le idonee **misure previste dall'art. 83** per il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale.

Tali misure sono costituite da:

Ordine di precedenza e di chiamata dei pazienti, prescindendo dalla loro individuazione nominativa e tenendo conto dell'eventuale uso di apparati vocali o di barriere.

Riservatezza nel momento del colloquio, prevenendo l'indebita venuta a conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute del paziente in visita. I locali scelti per tali prestazioni devono garantire detta riservatezza.

Richiesta agli incaricati amministrativi o di segreteria di attenersi a regole di condotta analoghe al segreto professionale.

5. Autorizzazione degli esercenti le professioni sanitarie diversi dai medici – art. 84

Sebbene di impatto specifico nel settore sanitario, si ricorda che in ottemperanza all'art. 84, che disciplina **la comunicazione dei dati relativi allo stato di salute del paziente**, il medico Titolare è tenuto ad autorizzare per iscritto, riportando le appropriate cautele imposte dal contesto, gli esercenti le professioni sanitarie diversi dai medici che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e di conseguenza trattano i dati relativi al loro stato di salute.

6. Le prescrizioni cartacee di medicinali non a carico del S.S.N. – artt. 88 e 89

Le generalità dell'interessato non devono essere indicate (art. 88). Il medico, tuttavia, è autorizzato a derogare a tale previsione quando ritenga indispensabile risalire all'identità dell'interessato per necessità derivante dalle sue particolari condizioni o da una speciale modalità di preparazione o di utilizzazione del farmaco.

7. Trattamento dei dati genetici - art. 90

Fino alla data in cui sarà efficace l'apposita Autorizzazione del Garante per il trattamento dei dati genetici prevista dall'art. 90 del Codice, restano autorizzati i trattamenti di tali dati nei soli limiti e alle condizioni individuate al punto 2, lett. b), dell'Autorizzazione n. 2/2002¹⁰ come contemplato dall'Autorizzazione n. 2/2004 al "trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale".

In tal senso, il trattamento di dati genetici è consentito limitatamente alle informazioni e alle operazioni indispensabili per tutelare l'incolumità fisica e la salute dell'interessato, di un terzo o della collettività, sulla base del consenso. In mancanza del consenso, se il trattamento è volto a tutelare l'incolumità fisica e la salute di un terzo o della collettività, questo può essere iniziato o proseguito solo previa apposita autorizzazione del Garante.

Qualora il trattamento riguardi informazioni di tipo genetico, l'informativa dovrà essere **integrata con ulteriori elementi** che saranno individuati proprio dalla prevista Autorizzazione.

In particolare, dovranno essere specificate le finalità perseguite e i risultati conseguibili, anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati, per consentire all'interessato di prendere una decisione libera e informata, ovvero per finalità probatorie in sede civile o penale, in conformità alla legge.

Ai sensi dell'art. 37, comma 1, è **soggetto a notifica il trattamento sistematico** di dati genetici o biometrici organizzati in una banca di dati ed accessibile a terzi per via telematica, effettuato dagli esercenti le professioni sanitarie - ad es. un genetista che tratta sistematicamente dati genetici - e dalle strutture sanitarie pubbliche e private - ad es. ospedali, case di cura e di riposo, aziende sanitarie, laboratori di analisi cliniche e associazioni sportive.

8. La notificazione - art. 37 per il trattamento dei dati genetici

La **notificazione** consiste nella comunicazione che il Titolare di un trattamento suscettibile di recare pregiudizio ai diritti e alla libertà dell'interessato deve inoltrare preventivamente al Garante dichiarando la sua intenzione di procedere a tale trattamento.

¹⁰ Autorizzazione n. 2/2002 autorizza il trattamento di dati genetici, limitatamente alle informazioni e alle operazioni indispensabili per tutelare l'incolumità fisica e la salute dell'interessato, di un terzo o della collettività, sulla base del consenso ai sensi degli articoli 22 e 23 della legge n. 675/1996. In mancanza del consenso, se il trattamento è volto a tutelare l'incolumità fisica e la salute di un terzo o della collettività, il trattamento può essere iniziato o proseguito solo previa apposita autorizzazione del Garante. I dati genetici non possono essere trattati dai soggetti di cui al punto 1.2, lettere c), d), e) ed f). Le informative all'interessato previste dall'art. 10 della legge n. 675/1996 devono porre in particolare evidenza il diritto dell'interessato di opporsi, per motivi legittimi, al trattamento dei dati genetici che lo riguardano. Fino alla data in cui sarà efficace l'apposita autorizzazione per il trattamento dei dati genetici prevista dall'art. 17, comma 5, del decreto n. 135/1999, e successive modificazioni ed integrazioni, i dati genetici trattati per fini di prevenzione, di diagnosi o di terapia nei confronti dell'interessato, ovvero per finalità di ricerca scientifica, possono essere utilizzati unicamente per tali finalità o per consentire all'interessato di prendere una decisione libera e informata, ovvero per finalità probatorie in sede civile o penale, in conformità alla legge.

E' escluso dalla notificazione - per effetto del **Provvedimento relativo ai casi da sottrarre all'obbligo di notificazione** del Garante - il trattamento **non sistematico** di dati genetici e biometrici effettuato sia individualmente sia eseguito in forma associata all'interno di uno stesso studio medico. Il trattamento di dati genetici, quindi, non va notificato **quando il professionista**, nell'ambito di ordinari rapporti con il paziente, viene a volte a conoscenza di informazioni di tipo genetico (ad es. in caso di indagini prenatali, diagnosi e cura di determinate patologie genetiche).

L'esonero però non opera per i trattamenti di dati genetici e biometrici **effettuati da strutture sanitarie pubbliche o private** (Ospedali, Case di cura e di riposo, Aziende sanitarie, Laboratori di analisi cliniche, Associazioni sportive).

9. Principio di necessità

L'art 91 del Codice stabilisce che il **trattamento**, in ogni forma, di **dati** idonei a rivelare lo stato di **salute** o la **vita sessuale** eventualmente **registrati su carte anche non elettroniche**, è **consentito solo nel rispetto del principio di necessità** fissato dall'art 3 del Codice.

Il **principio di necessità** prevede che i **sistemi informativi e i programmi informatici** (tra cui anche quelli che supportano l'utilizzo di carte elettroniche) devono essere **configurati riducendo al minimo l'utilizzo dei dati identificativi**, in modo da evitare che vengano trattati dati personali quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi o modalità tali da permettere l'identificazione dell'interessato solo in caso di necessità.

10. La cartella clinica – art. 92

L'esercente la professione medica o sanitaria in qualità di Titolare del trattamento **redige e conserva la cartella clinica in conformità alla disciplina** applicabile dettata dall'art. 92, vale a dire distinguendo i dati inerenti al paziente da quelli riguardanti altri interessati cui eventualmente si è accennato nelle anamnesi familiari.

In caso di controversia risarcitoria per danni ascritti all'attività professionale medica, documentata nella cartella clinica e prima della sua probabile acquisizione su iniziativa del giudice, è necessario procedere ad un'attenta valutazione dell'effettiva necessità di consentire l'accesso ad essa.

Referti e/o copie della cartella clinica saranno consegnati all'interessato – o ad un'altra persona però delegata per iscritto e munita della copia del documento d'identità dell'interessato – **in busta chiusa**, da parte del **personale amministrativo preposto** dal Titolare.

Oltre agli obblighi generali che impattano o possono impattare il medico esercente in regime di libera professione **esistono gli obblighi esecutivi**, cioè le **misure di sicurezza dei dati e dei sistemi**. Questi obblighi, commentati, sono **riportati nel documento relativo al Disciplinare Tecnico**.

Le sanzioni

Poiché la non ottemperanza degli obblighi indicati comporta sanzioni civili e penali, questo sunto conclude con un breve accenno puntuale delle sanzioni relative agli obblighi mancati.

L'**omessa o inidonea informativa** all'interessato costituisce una **violazione amministrativa** ed è punita con il pagamento di una somma **da tremila a diciottomila** euro nel caso si tratti di **dati personali comuni e identificativi**. Qualora si trattasse di **dati relativi alla salute**, la sanzione amministrativa va **dai cinquemila ai trentamila euro**. La **somma può essere aumentata sino al triplo** quando risulta inefficace in ragione delle condizioni economiche del contravventore (art. 161).

La **cessione dei dati**, in violazione di quanto previsto dall'art. 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali, è punita con la **sanzione amministrativa** del pagamento di una somma da cinquemila a trentamila euro. In questo ordine di idee, la violazione del art. 84, comma 1, inerente la **comunicazione dei dati** relativi alla salute al proprio interessato, è punita con il pagamento di una somma da cinquecento a tremila euro (art. 162).

Si incorre in **illeciti penali**, come indicato nell'art. 167, quando si effettua un **trattamento illecito di dati**: ad esempio la comunicazione o diffusione di dati relativi alla salute. Se dal fatto deriva danno, è punito con la reclusione da sei a venticinque mesi.

L'art. 169 indica che **chiunque, essendovi tenuto, omette di adottare le misure minime di sicurezza dei dati e dei sistemi** previste dall'art. 33 è punito con **l'arresto sino a due anni** o con **l'ammenda da diecimila a cinquantamila euro**.

L'art. 172 indica che la condanna per uno dei delitti previsti dal Codice in materia di protezione dei dati personali comporta la pubblicazione della sentenza.