

**Il Disciplinare Tecnico  
in materia di misure minime di sicurezza o Allegato B  
D.Lgs. n. 196/2003**

Commentato ad uso degli affiliati *hms*

Si tratta dell'insieme delle misure minime da adottare per la sicurezza dei dati a carattere personale, definite negli artt. 34-35 del Codice, per i trattamenti di dati personali eseguiti con o senza l'ausilio di strumenti elettronici. I dettagli realizzativi di tali misure vengono illustrati nel Disciplinare Tecnico.

Il Codice impone che i trattamenti che non osservino le misure indicate nel Disciplinare tecnico si ritengano non consentiti e soggetti a sanzioni penali.

L'art. 36 prevede che il Disciplinare venga aggiornato periodicamente dal Ministero della giustizia di concerto con il Ministero per l'innovazione e la tecnologia, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore. Ciò permette la revisione periodica delle misure senza un intervento legislativo sull'interezza del Codice.

Di seguito presentiamo una versione interpretata del Disciplinare Tecnico idoneo alla realtà dei professionisti affiliati ad *hms*, in quanto il Disciplinare tecnico costituisce una sorta di manuale che il Titolare, il responsabile (se designato) e l'incaricato del trattamento dei dati personali devono far proprio in modo che le mansioni e l'operato possano essere soggetti a verifica e di evitare di incorrere in trattamenti non consentiti.

Il **Disciplinare Tecnico** illustra le **modalità** tecniche da adottare a cura del **Medico Chirurgo o Veterinario Titolare** oppure dall'eventuale **Responsabile** (ove designato) e dalla **Segretaria Incaricata**, in caso di trattamento con o senza l'ausilio di strumenti elettronici.

❖ **Trattamento CON l'ausilio di strumenti elettronici (punti dal 1 al 26)**

- Sistema di autenticazione informatica.
- Sistema di autorizzazione.
- Altre misure di sicurezza tra cui il Documento Programmatico sulla Sicurezza (DPS).
- Misure del trattamento dei dati sensibili o giudiziari.
- Misure di tutela e garanzia.

❖ **Trattamento SENZA l'ausilio di strumenti elettronici (punti dal 27 al 29)**

- Istruzioni scritte alle **Segretarie**.
- Affidamento di atti e documenti.
- Accesso controllato agli archivi.

## Trattamento con l'ausilio di strumenti elettronici

### Sistema di autenticazione informatica

La fase di autenticazione è quella in cui il sistema provvede all'identificazione certa dell'utente mediante un sistema di riconoscimento (*user mane, log in*) che lo individua univocamente come utente noto al sistema. Il tal senso bisogna tener presente le seguenti misure.

1. Il trattamento di dati personali con strumenti elettronici è consentito soltanto all'incaricato (segretaria) dotato di **credenziali di autenticazione**.
2. Queste consistono, per esempio, in un codice (*user id*) che identifica l'incaricato (segretaria) associato a una parola chiave (password) riservata, conosciuta solamente dal medesimo, o ad altri dispositivi di autenticazione.
3. Ad ogni incaricato (segretaria) devono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Le istruzioni impartite all'incaricato (segretaria) devono prescrivere l'adozione di cautele che assicurino la segretezza delle credenziali di autenticazione e la conservazione diligente di eventuali dispositivi necessari per l'autenticazione.
5. La password, quando è prevista dal sistema di autenticazione, deve essere composta da almeno 8 (otto) caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Si suggerisce agli utenti di non utilizzare riferimenti facilmente riconducibili ai propri dati identificativi. La password che viene assegnata deve essere modificata al primo utilizzo e, successivamente, almeno ogni sei mesi (\*).

(\*). In caso di trattamento di dati relativi alla salute dei pazienti, invece, la password deve essere modificata almeno ogni tre mesi. **Nel caso di accesso a tali dati da parte della segretaria bisogna definire quali operazioni è autorizzata ad eseguire e renderlo noto nell'atto di nomina.**

6. Un codice già utilizzato da un incaricato non deve essere assegnato ad un altro neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali devono essere disattivate anche in caso di perdita delle caratteristiche che consentono all'incaricato (segretaria) l'accesso ai dati personali.
9. Devono essere impartite istruzioni all'incaricato (Segretaria) per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. In previsione di prolungata assenza o impedimento dell'incaricato che rende indifferibile il ripristino delle operatività del sistema, il **Medico Titolare è tenuto** ad adottare disposizioni scritte per la modalità di ripristino. In tal caso subentra l'individuazione per iscritto dell'incaricato che assumerà la responsabilità, compresa la custodia delle copie delle credenziali di autenticazione.
11. Le disposizioni sul sistema di autenticazione di cui ai punti precedenti e quelle sul sistema di autorizzazione, non si applicano ai trattamenti dei dati personali destinati alla diffusione.

## Sistema di autorizzazione

Il Disciplinare distingue tra sistema di **autenticazione** e sistema di **autorizzazione**: due operazioni ben diverse e non intercambiabili. Un utente che si presenta ad un sistema informatico viene dapprima autenticato, poi, quando richiede determinati servizi – per esempio l'accesso a un database o ad una risorsa -, viene di volta in volta autorizzato. L'autorizzazione è la fase in cui il sistema concede o non concede, ad un utente già autenticato, l'accesso a determinati dati o programmi in funzione del suo profilo.

Le misure previste per il sistema di autorizzazione sono di grande semplicità.

12. Viene utilizzato un sistema di autorizzazione quando per gli incaricati (diverse segretarie) sono individuati **profili di autorizzazione** di ambito diverso.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, devono essere individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le relative operazioni di trattamento, evitando sconfinamenti oltre i limiti dell'incarico.
14. Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
15. In sede di aggiornamento degli ambiti di trattamento assegnati ai singoli operatori, la lista degli incaricati (segretarie) può essere redatta anche per classi omogenee in quanto condividono i profili di autorizzazione.

## Altre misure di sicurezza

Nel Disciplinare sono contemplate ulteriori misure minime di sicurezza per prevenire trattamenti illeciti e accessi non consentiti.

16. I dati personali devono essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies<sup>1</sup> del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale. Si tratta di opportuni **antivirus** aggiornabili con **cadenza almeno semestrale**.
17. Gli aggiornamenti periodici dei **programmi per elaboratore**, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, devono essere effettuati almeno annualmente. In caso di trattamento di **dati sensibili** o giudiziari l'aggiornamento deve essere **almeno semestrale**.
18. Devono essere impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

---

<sup>1</sup> **Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.** Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire 20 milioni".

## Documento Programmatico sulla Sicurezza

19. Entro il 31 marzo di ogni anno, il **Medico Titolare** di trattamenti sistematici di dati sensibili con strumenti elettronici (server, workstation oppure PC), deve **redigere un Documento Programmatico sulla Sicurezza (DPS), cioè delineare la strategia di sicurezza complessiva che si intende adottare al fine di ottemperare agli obblighi generali previsti dal Codice** (artt. 3 e 31), contenente idonee informazioni a riguardo:

- Elenco dei trattamenti di dati personali
- Distribuzione dei compiti e delle responsabilità
- Analisi dei rischi che incombono sui dati
- Misure in essere e da adottare
- Criteri e modalità di ripristino della disponibilità dei dati
- Pianificazione degli interventi formativi previsti
- Trattamento affidati all'esterno
- Cifratura dei dati sensibili o separazione mediante codice dei dati identificativi

## Misure del trattamento dei dati sensibili

20. I dati sensibili devono essere protetti contro l'accesso abusivo, di cui all'art.615-ter<sup>2</sup> del Codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Devono essere 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 informazione relativa alla salute dei paziente, se non utilizzati, devono essere distrutti o resi inutilizzabili. Tale processo ha il compito di impedire che personale non autorizzato venga a conoscenza dei dati contenuti nei supporti rimovibili nel caso vengano riutilizzati.

23. Devono essere 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 dei pazienti e non superiori a 7 (sette) giorni.

24. I dati relativi alla salute contenuti in elenchi, registri o banche dati, devono essere tenuti disgiunti dai dati identificativi mediante tecniche di cifratura o con l'utilizzazione di codici. La soluzione tecnica adottata deve rendere i dati sensibili temporaneamente intelligibili anche a chi è autorizzato ad accedervi, limitando l'identificazione degli interessati solo al caso di necessità (come disciplinato dall'articolo 22, comma 6). I dati relativi all'identità genetica devono essere trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve

---

<sup>2</sup> Il reato di "**accesso abusivo ad un sistema informatico o telematico**" all'art.615-ter recita testualmente: "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto di escluderlo, è punito con la reclusione fino a tre anni". Seguono delle ipotesi aggravate a seconda che il soggetto agente rivesta una determinata qualifica (es. Pubblico Ufficiale), o se si è usata violenza, o ancora se dal fatto deriva distruzione o danneggiamento del sistema.

avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

### Misure di tutela e garanzia della trasparenza dei rapporti con l'esterno e con soci

25. Il **Medico 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 **Medico Titolare** riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del Documento Programmatico sulla Sicurezza.

### Trattamento senza l'ausilio di strumenti elettronici

Il Disciplinare Tecnico stabilisce che il trattamento di dati personali eseguito senza l'ausilio di strumenti elettronici sia consentito solo se vengono adottate le seguenti misure.

#### Istruzioni scritte

27. All'incaricato (segretaria) 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 i dati personali. Nell'ambito dell'**aggiornamento** periodico con cadenza almeno annuale nell'individuazione dell'**ambito del trattamento** consentito, la lista degli incaricati (segretarie) può essere redatta anche in presenza di classi omogenee e dei relativi profili di autorizzazione.

#### Durata del trattamento

28. Quando gli **atti** e i **documenti** contenenti **dati** personali **sensibili** sono **affidati** all'incaricato (segretaria) per lo **svolgimento** dei relativi **compiti**, i medesimi atti e documenti sono **controllati e custoditi** dallo stesso fino alla **restituzione**, in maniera che ad essi non accedano persone prive di autorizzazione. La restituzione avviene **al termine** delle operazioni affidate.

#### Controllo di accesso agli archivi

29. L'**accesso** agli **archivi** contenenti **dati sensibili** deve essere **controllato**. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere 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 devono essere preventivamente autorizzate.