

Misure minime di sicurezza per il trattamento dei dati personali

- [Decreto del Presidente della Repubblica 28 luglio 1999, n. 318](#)
Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge
31 dicembre 1996, n. 675
- [Legge del 3 novembre 2000 n. 325](#)
Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della legge 31 dicembre 1996, n. 675
- [Documento programmatico sulla sicurezza: istruzioni](#)
- [Documento programmatico sulla sicurezza: autorizzazioni](#)

Decreto del Presidente della Repubblica 28 luglio 1999, n. 318 Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675

Preambolo

IL PRESIDENTE DELLA REPUBBLICA

Visto l'articolo 87, comma quinto, della Costituzione;

Visto l'articolo 15 della legge 31 dicembre 1996, n. 675, recante «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»;

Ritenuto che ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675, occorre individuare, in via preventiva, le misure minime di sicurezza per i dati personali oggetto di trattamento, al fine di assicurare il funzionamento delle misure sanzionatorie penali previste dall'articolo 36 della medesima legge;

Visto l'articolo 17, comma 1, lettera a), della legge 23 agosto 1988, n. 400;

Sentiti l'Autorità per l'informatica nella pubblica amministrazione e il Garante per la protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 26 aprile 1999;

Ritenuto di dover comunque garantire la possibilità, in caso di più incaricati del trattamento, di limitare l'accesso a determinati dati personali attraverso la previsione di una specifica parola chiave per tali dati, senza operare, quindi, alcuna equiparazione tra tale ipotesi e quella relativa alla previsione di un'unica parola chiave per l'accesso al sistema; Viste le deliberazioni del Consiglio dei Ministri, adottate nelle riunioni del 16 luglio e del 23 luglio 1999; Sulla proposta del Ministro di grazia e giustizia;

EMANA

il seguente regolamento:

CAPO I - PRINCIPI GENERALI

Art. 1- Definizioni

1. Ai fini del presente regolamento si applicano le definizioni elencate nell'articolo 1 della legge 31 dicembre 1996, n. 675, di seguito denominata legge. Ai medesimi fini si intendono per:

- a) «misure minime»: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel presente regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'articolo 15, comma 1, della legge;
- b) «strumenti»: i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento;
- c) «amministratori di sistema»: i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

CAPO II - TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI

Sezione I - Trattamento dei dati personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali

Sezione I - Trattamento dei dati personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali**Art. 2 - Individuazione degli incaricati**

1. Salvo quanto previsto dall'articolo 8, se il trattamento dei dati personali è effettuato per fini diversi da quelli di cui all'articolo 3 della legge mediante elaboratori non accessibili da altri elaboratori o terminali, devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure:

- a) prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti ai sensi della lettera b);
- b) individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.

CAPO II - TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI**Sezione II - Trattamento dei dati personali effettuato mediante elaboratori accessibili in rete****Art. 3 - Classificazione**

1. Ai fini della presente sezione gli elaboratori accessibili in rete impiegati nel trattamento dei dati personali sono distinti in:

- a) elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico;
- b) elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.

Art. 4 - Codici identificativi e protezione degli elaboratori

1. Nel caso di trattamenti effettuati con gli elaboratori di cui all'articolo 3, oltre a quanto previsto dall'articolo 2 devono essere adottate le seguenti misure:

- a) a ciascun utente o in caricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse;
- b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi;
- c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.

2. Le disposizioni di cui al comma 1, lettere a) e b), non si applicano ai trattamenti dei dati personali di cui è consentita la diffusione.

Art. 5 - Accesso ai dati particolari

1. Per il trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato ai sensi dell'articolo 3, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Se il trattamento è effettuato ai sensi dell'articolo 3, comma 1, lettera b), sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico.

2. L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.

3. Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.

4. L'autorizzazione all'accesso deve essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.

5. La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso.

6. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

7. Le disposizioni di cui ai commi da la 6 non si applicano al trattamento dei dati personali di cui è consentita la diffusione.

Art. 6 - Documento programmatico sulla sicurezza

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato mediante gli elaboratori indicati nell'articolo 3, comma 1, lettera b), deve essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

- a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi;
- b) i criteri e le procedure per assicurare l'integrità dei dati;
- c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica;
- d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.

2. L'efficacia delle misure di sicurezza adottate ai sensi del comma 1 deve essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

Art. 7. - Reimpiego dei supporti di memorizzazione

1. Nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato con gli strumenti di cui all'articolo 3, i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.

CAPO II - TRATTAMENTO DEI DATI PERSONALI EFFETTUATO CON STRUMENTI ELETTRONICI O COMUNQUE AUTOMATIZZATI

Sezione III - Trattamento dei dati personali effettuato per fini esclusivamente personali

Art. 8 - Parola chiave

1. Ai sensi dell'articolo 3 della legge, il trattamento per fini esclusivamente personali dei dati di cui agli articoli 22 e 24 della legge, effettuato con elaboratori stabilmente accessibili da altri elaboratori, è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati.

CAPO III - TRATTAMENTO DEI DATI PERSONALI CON STRUMENTI DIVERSI DA QUELLI ELETTRONICI O COMUNQUE AUTOMATIZZATI

Art. 9 - Trattamento di dati personali

1. Nel caso di trattamento di dati personali per fini diversi da quelli dell'articolo 3 della legge, effettuato, con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalità:
- a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli articoli 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
 - b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.
2. Nel caso di trattamento di dati di cui agli articoli 22 e 24 della legge, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità:
- a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura;
 - b) l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

Art. 10 - Conservazione della documentazione relativa al trattamento

1. I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui agli articoli 22 e 24 della legge devono essere conservati e custoditi con le modalità di cui all'articolo 9. Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 28 luglio 1999

CIAMPI

D'Alema, Presidente del Consiglio dei Ministri

Diliberto, Ministro di grazia e giustizia

Visto, il Guardasigilli: Diliberto



**Legge del 3 novembre 2000 n. 325
Disposizioni inerenti all'adozione delle misure minime di sicurezza nel
trattamento dei dati personali previste dall'articolo 15 della legge 31
dicembre 1996, n. 675**

**Art. 1 - Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati
personali previste dall'articolo 15 della legge 31 dicembre 1996, n. 675**

1. In sede di prima applicazione della disciplina contenuta nell'[articolo 15 della legge 31 dicembre 1996, n. 675](#), le misure di sicurezza di cui al [decreto del Presidente della Repubblica 28 luglio 1999, n. 318](#), possono essere adottate entro il 31 dicembre 2000 dai soggetti che documentino per iscritto le particolari esigenze tecniche e organizzative che rendono necessario avvalersi di un termine più ampio di quello previsto dall'[articolo 41, comma 3, della medesima legge n. 675 del 1996](#).
2. Il documento di cui al comma 1 deve essere redatto entro un mese dalla data di entrata in vigore della presente legge con atto avente data certa e deve contenere una esposizione sintetica delle informazioni necessarie, da cui risultino:
 - a) gli accorgimenti da adottare o già adottati e gli elementi che caratterizzano il programma di adeguamento, nonché le singole fasi in cui esso è eventualmente ripartito;
 - b) le linee-guida previste per dare piena attuazione alle misure minime di sicurezza, la cui inosservanza è sanzionata ai sensi dell'[articolo 36 della legge 31 dicembre 1996, n. 675](#), nonché alle più ampie misure di sicurezza previste dal [comma 1 dell'articolo 15 della medesima legge n. 675 del 1996](#).
3. Il documento di cui ai commi 1 e 2 deve essere conservato presso di sé a cura del soggetto interessato.
4. La violazione di uno degli obblighi di cui ai commi 2 e 3 comporta l'inapplicabilità di quanto previsto al comma 1.



Documento programmatico sulla sicurezza: istruzioni

"....gli atti previsti dal regolamento, come il documento programmatico sulla sicurezza o la designazione dei responsabili e degli incaricati del trattamento,devono essere esibiti all'Autorità solo a seguito di una eventuale e specifica richiesta in sede di ispezione o di controllo."
Vanno quindi conservati nello studio e non spediti al Garante nè a nessun altro.

Il Documento programmatico sulla sicurezza o "piano sicurezza" è stato redatto tenuto conto delle caratteristiche del SW del Co.S. ovvero Koinè 1.x e Koinè 2

Medico che usa cartelle cliniche cartacee	Disposizioni	Piano sicurezza
Medico che usa cartelle cliniche informatizzate su computer non collegato a rete locale o pubblica	Disposizioni	Piano sicurezza
Medici che usano cartelle cliniche informatizzate su computer accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico es. medicina di gruppo	Disposizioni	Piano sicurezza - senza server - con server

Medici che usano cartelle cliniche informatizzate su computer accessibili mediante una rete di telecomunicazioni disponibili al pubblico es. medicina in rete geografica (WAN)	Disposizioni	Piano sicurezza
---	------------------------------	---------------------------------

Medico che usa cartelle cliniche cartacee

Le cartelle devono essere chiuse a chiave in uno schedario dotato di serratura se ai locali accedono persone diverse dal medico titolare, (anche solo l'addetto alle pulizie o parenti del medico). La chiave deve essere custodita dal titolare.

Qualora il medico si avvalga della collaborazione di personale di segreteria o di sostituti, questi soggetti devono essere autorizzati per scritto, specificando per quali competenze sono autorizzati a consultare le cartelle (la/e lettera/e deve essere conservata dal titolare e dagli interessati ed essere disponibile nello studio per eventuali controlli - non deve essere timbrata alla posta o autenticata dal notaio, ne spedita al garante).

Su un altro foglio conservato nello studio devono essere identificate le altre persone che accedono ai locali dopo l'orario di chiusura, anche se non sono autorizzati a prendere visione delle cartelle.

Questi documenti ovviamente devono essere rifatti ogni volta che cambiano le persone e comunque almeno una volta all'anno.

Medico che usa cartelle cliniche informatizzate su computer non collegato a rete locale o pubblica

Deve essere previsto un salvataggio periodico dei dati (tutti dovrebbero già provvedere al backup periodico).

Deve essere prevista una parola chiave per l'accesso al computer o al programma contenente i dati.

NB

il medico compilerà il proprio documento programmatico individuale relativo alla sicurezza del suo computer

Medici che usano cartelle cliniche informatizzate su computer collegati ad una rete locale LAN: medicina di gruppo

Deve essere previsto un salvataggio periodico dei dati (tutti dovrebbero già provvedere al backup periodico).

Deve essere installato un software antivirus (registrato) aggiornato almeno ogni sei mesi.

Deve essere prevista una parola chiave diversa per ogni persona autorizzata a collegarsi alla rete (Colleghi, segretarie, infermieri, ecc.)

Uno dei titolari deve assumere il ruolo di amministratore di sistema che assegna e conserva le parole chiave di accesso di tutte le persone autorizzate.

L'amministratore di sistema deve provvedere a rimuovere la parola chiave e l'autorizzazione all'accesso qualora il soggetto non sia più autorizzato o non acceda all'elaboratore per più di sei mesi.

Il titolare dei dati (in pratica ciascun medico per le sue cartelle) deve autorizzare per scritto la altre persone che devono trattare i dati, specificando per quali competenze sono autorizzati). In caso di più medici nello stesso studio, ciascun medico deve autorizzare gli altri con la stessa procedura. Tali documenti devono essere conservati dai titolari e dagli interessati ed essere disponibili nello studio per eventuali controlli – non devono essere timbrati alla posta o autenticati dal notaio, ne spediti al garante.

Questi documenti devono ovviamente essere rifatti ogni volta che cambiano le persone e comunque almeno una volta all'anno.

NB:

- 1) nel modello di rete senza server (ogni computer di ogni medico contiene gli archivi di quel medico)
 - ogni medico compilerà il proprio documento programmatico individuale relativo alla sicurezza del suo computer
 - l'amministratore di sistema compilerà il documento programmatico relativo alla sicurezza della rete
- 2) nel modello di rete con server (che contiene gli archivi di tutti i medici)
 - solo l'amministratore di sistema compilerà il documento programmatico relativo alla sicurezza della rete

Medici che usano cartelle cliniche informatizzate su computer collegati ad una rete geografica WAN: medicina in rete

Oltre a ciò che è stato specificato per i medici che lavorano in rete locale, i colleghi che si trovano in questa condizione devono predisporre e aggiornare con cadenza annuale un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi:

- a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.
- b) I criteri e le procedure per assicurare l'integrità dei dati
- c) I criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per la restrizione dell'accesso per via telematica.
- d) L'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

NB

nel modello di rete geografica (ogni computer di ogni medico contiene gli archivi di quel medico) ed esiste
 un server remoto di rete che contiene una copia aggiornata degli archivi di ogni medico

- ogni medico compilerà il proprio documento programmatico individuale relativo alla sicurezza del suo computer
- l'amministratore di sistema compilerà il documento programmatico relativo alla sicurezza della rete

Autorizzazioni

Medico con collaboratore di studio o infermiera

Se nello studio ci sono segretarie od altri medici che devono avere accesso al programma ed ai dati per le loro funzioni, il titolare deve autorizzarli per scritto specificando per quali competenze sono autorizzati a consultare le cartelle (la/e lettera/e deve essere conservata dal titolare e dagli interessati ed essere disponibile nello studio per eventuali controlli - non deve essere timbrata alla posta o autenticata dal notaio, né spedita al garante).

Questi documenti devono essere rifatti ovviamente ogni volta che cambiano le persone e comunque almeno una volta all'anno

[modello per infermiera/e](#)

[modello per collaboratore di studio](#)

Rapporti con medici sostituti

Valgono le regole descritte per il personale di studio. Il collega va autorizzato per iscritto, il foglio va tenuto presso lo studio e rifatto ogniqualvolta cambi il collega sostituto.

[modello per altro medico](#)

Nomina amministratore di rete

Nelle forme associative "Medicina di Gruppo" e "Medicina in rete" deve essere nominato un Amministratore di sistema

[modello per la nomina dell' amministratore di sistema](#)