I . DEFINIZIONI contenute nell' art 4 del Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"

1. Ai fini del presente codice si intende per:

a) ***"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 di dati;

b) ***"dato personale"***, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) ***"dati identificativi"***, i dati personali che permettono l'identificazione diretta dell'interessato;

d) ***"dati sensibili"***, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonche' i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

e) ***"dati giudiziari"***, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualita' di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) ***"titolare"***, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalita', alle modalita' del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) ***"responsabile"***, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) ***"incaricati"***, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) ***"interessato"***, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) ***"comunicazione"***, il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) ***"diffusione"***, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) ***"dato anonimo"***, il dato che in origine, o a seguito di trattamento, non puo' essere associato ad un interessato identificato o identificabile;

o) ***"blocco"***, la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) ***"banca di dati"***, qualsiasi complesso organizzato di dati personali, ripartito in una o piu' unita' dislocate in uno o piu' siti;

q) ***"Garante"***, l'autorita' di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675,

2. Ai fini del presente codice si intende, inoltre, per:

a) ***"comunicazione elettronica"***, ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) ***"chiamata"***, la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) ***"reti di comunicazione elettronica"***, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) ***"rete pubblica di comunicazioni"***, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) ***"servizio di comunicazione elettronica"***, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) ***"abbonato"***, qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) ***"utente"***, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) ***"dati relativi al traffico"***, qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) ***"dati relativi all'ubicazione"***, ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) ***"servizio a valore aggiunto"***, il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) ***"posta elettronica"***, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresi', per:

a) ***"misure minime"***, il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) ***"strumenti elettronici"***, gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) ***"autenticazione informatica"***, l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identita';

d) ***"credenziali di autenticazione"***, i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e) ***"parola chiave"***, componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) ***"profilo di autorizzazione"*** , l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa puo' accedere, nonche' i trattamenti ad essa consentiti;

g) ***"sistema di autorizzazione"***, l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalita' di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:

a) ***"scopi storici"***, le finalita' di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) ***"scopi statistici"***, le finalita' di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) ***"scopi scientifici"***, le finalita' di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

II . ADEMPIMENTI nei confronti dei CLIENTI - UTENTI

1. DATI PERSONALI di tipo GENERICO (quali ad esempio - data e luogo di nascita - residenza, domicilio o recapito - professione - codice fiscale e/o partita I.V.A. - nazionalità - numero di telefono o di fax o indirizzo di posta elettronica). In base all'art. 23 del D.Lgs.n.196/2003 il trattamento dei dati personali da parte di soggetti privati è ammesso solo con il consenso espresso dell'interessato (e cioè del "cliente-utente"). Il consenso è validamente prestato solo se è espresso liberamente, in forma specifica e documentata per iscritto, e se sono state date all'interessato (cliente-committente) - per iscritto ovvero verbalmente - le seguenti informazioni (art. 13 del D.Lgs. 196/2003):

- sulle finalità (per l'espletamento dell'incarico professionale) e modalità del trattamento cui sono destinati i "dati personali";

- sulla necessità del conferimento di tutti quei dati che sono indispensabili per l'assolvimento dell'incarico professionale;

- circa l'ambito professionale di comunicazione o diffusione dei dati stessi;

- sui diritti dell'interessato (cliente-utente) circa il trattamento dei suoi dati personali: diritti elencati nell'art. 7 del D.Lgs. 196/2003 - vedi schema pubblicato di seguito.

- il nome e l'indirizzo del "responsabile" - ove sia una persona diversa dal libero professionista quale "titolare" dei dati - del trattamento dei dati.

2. DATI PERSONALI definiti "SENSIBILI".

Con provvedimento n. 4/2000 emesso in data 20.09.2000 dal "Garante" (e pubblicato sul n.229 della "Gazzetta ufficiale" del 30.09.2000) i liberi professionisti iscritti in Albi o Elenchi professionali sono stati AUTORIZZATI in via generale - dal 01 ottobre 2000 fino al 31 dicembre 2001 - a trattare i "dati sensibili" di cui all'art. 22, comma 1°, della legge n. 675/1996. Per gli Psicologi assume particolare rilievo il provvedimento n. 2/2000 emesso in data 20.09.2000 dal "Garante" (e pubblicato sul n. 229 della "Gazzetta ufficiale" del 30.09.2000) con il quale si prevede che l' autorizzazione al trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale "è rilasciata, anche senza richiesta: a) ai medici-chirurghi, ai farmacisti, agli odontoiatri, agli psicologi e agli altri esercenti le professioni sanitarie iscritti in albi o in elenchi".

Si precisa che "in tali casi l' autorizzazione è rilasciata al fine di consentire ai destinatari di adempiere o di esigere l' adempimento di specifici obblighi o di eseguire specifici compiti previsti da leggi, dalla normativa comunitaria o da regolamenti (…) .
Il trattamento può riguardare anche la compilazione di cartelle cliniche, di certificati e di altri documenti relativi alla gestione amministrativa la cui utilizzazione sia necessaria per i fini suindicati".

Avuto riguardo a quanto sopra indicato è quindi NECESSARIO che lo Psicologo faccia sottoscrivere al proprio cliente all'atto del conferimento dell'incarico professionale - una INFORMATIVA/DICHIARAZIONE AUTORIZZATORIA (che esprima cioè il suo consenso) al trattamento sia dei DATI di tipo GENERICO, sia di quelli considerati "SENSIBILI".

I moduli per richiedere il consenso informato sono disponibili sul sito web dell'Ordine degli Psicologi dell'Emilia Romagna nella sezione PRIVACY/Modulistica.

III . ADEMPIMENTI nei confronti dei COLLABORATORI e/o DIPENDENTI del professionista e nei confronti dei fornitori.

In relazione a quanto disposto dai PROVVEDIMENTI n. 01/2000 e n. 04/2000 emessi in data 20.09.2000 dall'"Autorità per la protezione dei dati personali" in merito al trattamento dei "DATI SENSIBILI" nei RAPPORTI di LAVORO (provvedimenti pubblicati nel n. 229 della "Gazzetta ufficiale" del 30.09.2001) **è necessario acquisire dai COLLABORATORI e dai DIPENDENTI il loro consenso scritto all'utilizzo ed al trattamento dei loro DATI PERSONALI sia di tipo generico che classificati come "sensibili".** Il provvedimento n. 01/2000 del 20.09.2000 autorizza in via generale il trattamento dei "dati sensibili" nei rapporti di lavoro, secondo le prescrizioni ivi indicate. Il testo del consenso da far sottoscrivere può essere analogo (previ opportuni adattamenti) a quello dello schema per i clienti-utenti.

Il modulo per la comunicazione da inviare ai fornitori è disponibile sul sito web dell'Ordine degli Psicologi dell'Emilia Romagna alla voce PRIVACY/Modulistica.

IV . ADEMPIMENTI con riguardo all'UTILIZZO del FAX e/o della POSTA TELEMATICA.

Nei FAX e nella cd. POSTA TELEMATICA (per l'invio di "e-mail") è consigliabile inserire - in calce - la seguente AVVERTENZA: "Questo messaggio è destinato unicamente alla/e persona/e sopraindicata/e. E' strettamente personale e può contenere informazioni la cui riservatezza è tutelata dalla normativa sulla cd. "privacy". E' espressamente vietato alla/e persona/e non destinataria/e leggere, copiare o comunque usare questo messaggio o diffonderne il contenuto senza autorizzazione. Chi ha ricevuto per errore questo fax o messaggio è pregato di distruggerlo e di avvertire per telefono o fax o "e-mail", il mittente."

V . ADOZIONE di "MISURE MINIME di SICUREZZA" nel TRATTAMENTO dei DATI PERSONALI.

1. FONTI NORMATIVE:

- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" pubblicato nella Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123 : artt. 31 e seguenti ed Allegato B (DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA).

2. DEFINIZIONI

Art. 31- Obblighi di sicurezza
1. 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 o di trattamento non consentito o non conforme alle finalita' della raccolta.

3. MISURE MINIME DI SICUREZZA

Art. 33 - Misure minime
1. Nel quadro dei piu' generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34 - Trattamenti con strumenti elettronici
1. Il trattamento di dati personali effettuato con strumenti elettronici e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilita' dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitart.

Art. 35 - Trattamenti senza l'ausilio di strumenti elettronici
1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici e' consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unita' organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalita' di accesso finalizzata all'identificazione degli incaricati.

Art. 36 - Adeguamento
1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, e' aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

4. ALLEGATO B - DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

Artt. da 33 a 36 del codice - Trattamenti con strumenti elettronici
Modalita' 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 e' 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 piu' credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati e' 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 e' prevista dal sistema di autenticazione, e' 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 e' 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 e' modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non puo' 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 qualita' 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 e' consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalita' con le quali il titolare puo' assicurare la disponibilita' di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessita' di operativita' e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali e' 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 e' 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, e' 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 puo' 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 vulnerabilita' di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento e'

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 responsabilita' 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'integrita' e la disponibilita' dei dati, nonche' la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilita';
19.5. la descrizione dei criteri e delle modalita' per il ripristino della disponibilita' 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 piu' rilevanti in rapporto alle relative attivita', delle responsabilita' che ne derivano e delle modalita' per aggiornarsi sulle misure minime adottate dal titolare. La formazione e' programmata gia' al momento dell'ingresso in servizio, nonche' 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 conformita' 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 modalita' 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'identita' 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 e' 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 conformita' 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. Modalita' 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 puo' 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 e' 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.