Studio Medico Corso Comandini

INDICE

DOCUMENTO PROGRAMMATICO

E DELLE PROCEDURE DI SALVAGUARDIA DEI DATI E DELLA PRIVACY

TITOLARI DEL TRATTAMENTO:

1. AnnaMaria Amaducci

   ◊ città: Cesena
   ◊ provincia: FC
   ◊ cap: 47023
   ◊ indirizzo: Corso U.Comandini 12/b
   ◊ partita iva: 00743510406

2. Alberto Forgiarini

   ◊ città: Cesena
   ◊ provincia: FC
   ◊ cap: 47023
   ◊ indirizzo: Corso U. Comandini 12/b
   ◊ partita iva: 00950630400

3. Michele Marcatelli

   ◊ città: CEsena
   ◊ provincia: FC
   ◊ cap: 47023
   ◊ indirizzo: Corso U. Comandini 12/b
   ◊ partita iva: 01410550402

Se il responsabile del trattamento non viene designato, i titolari sono tutti responsabili del trattamento.

SCOPO DEL REGOLAMENTO E DEL DOCUMENTO PROGRAMMATICO

Il titolare del trattamento, al fine di gestire correttamente gli adempimenti connessi alla legge e per creare e sostenere una cultura della privacy, ha predisposto il presente regolamento al fine di definire le responsabilità, le procedure, le azioni per la gestione dei rischi e per l'adozione delle misure di sicurezza imposte dalle legge. Il manuale, inoltre, ha lo scopo di creare regole a rilevanza interna ed esterna utili e/o necessarie per garantire i diritti dei titolari dei dati ed a salvaguardia del patrimonio informativo. La corretta applicazione delle misure di sicurezza consente non solo di adempiere agli obblighi di legge, ma anche di migliorare l'organizzazione ottimizzando i processi di lavoro ed operare nella consapevolezza che i dati trattati siano corretti, integri, aggiornati – come richiesto dal Codice all'art. 11 − e costituiscano, perciò, un vero patrimonio della professione.

MISURE DI SICUREZZA IDONEE E RESPONSABILITA' CIVILE DEL TITOLARE DEL TRATTAMENTO

Le misure di sicurezza "minime" sono solo una parte degli accorgimenti obbligatori in materia di sicurezza (art. 33 del Codice). Esiste un obbligo più generale di ridurre al minimo determinati rischi, per cui occorre custodire e controllare i dati personali oggetto di trattamento per contenere le probabilità che i dati siano distrutti, dispersi, anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito. Ciò va fatto adottando misure idonee anche in base al progresso tecnico, alla natura dei dati ed alla caratteristiche del trattamento. L'inosservanza di quest'obbligo rende il trattamento illecito, anche se non si determina un danno per gli interessati; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice). Tali misure di sicurezza "idonee" sono individuate dal Titolare sulla base di un'analisi specifica delle proprie caratteristiche tecnologiche, organizzative e di processo, tenuto conto delle "innovazioni tecnologiche" e delle soluzioni di sicurezza offerte dal mercato. E' obbligo dotarsi degli strumenti più idonei in relazione ai mutati rischi ed all'evoluzione tecnologica dei sistemi di protezione dei dati. Con il presente documento verrà adottata anche idonea modulistica al fine di dare istruzioni precise al personale ed informazioni chiare sulle garanzie della corretta gestione dei dati.

PRINCIPALI DEFINIZIONI

Per sistema informativo l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti all'attività esercitata. I dati personali contenuti nel sistema informativo devono essere

protetti adottando le misure minime di sicurezza previste dal D. Lgs. 196/2003 “Codice in materia di protezione dei dati personali” (d’ora in poi codice) artt. 33−36, con le modalità descritte dal disciplinare tecnico allegato B al codice stesso.

AI FINI DEL D. LGS. 196/2003 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, nonché 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 qualità 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 finalità, alle modalità 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 o giuridiche 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;

j) "comunicazione", il dare conoscenza dei dati personali a uno o più 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;

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

l) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

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

n) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

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

AI FINI DEL D. LGS. 196/2003 IN RIFERIMENTO ALLA SICUREZZA DEI DATI:

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'identità;

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 può accedere, nonché i trattamenti ad essa consentiti;

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

DEFINIZIONE DEI RUOLI NELLA GESTIONE DEI DATI

Il titolare, svolge le funzioni di “titolare del trattamento dei dati personali” le più opportune modalità di trattamento e gli strumenti da utilizzare, ivi compreso il profilo della sicurezza. E’ previsto, inoltre, che le decisioni possano essere prese anche unitamente ad altro titolare (art. 4 lett. f) del codice).

Il Titolare del trattamento dei dati:

> adotta (art. 31 “codice”), riguardo al trattamento di dati personali, le misure minime di sicurezza (art. 33 “codice”) con le modalità previste dal Titolo V, Capo II del “codice” e dal disciplinare tecnico contenuto nell’allegato B) del “codice” stesso;

> adotta il documento programmatico della sicurezza entro il 31 marzo di ogni anno, ai sensi della regola 19 all. B del codice, vigilando sulla sua effettiva applicazione.

> adotta ove necessario le misure minime di sicurezza avvalendosi anche di soggetti esterni alla propria struttura, ricevendo dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico; allegato al “codice” (art. 25 all. B “codice”);

> verifica l’adeguamento delle misure minime di sicurezza previste per la protezione dei dati personali e provvede all’aggiornamento periodico predisposto dal 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 (art. 36 del “codice”).

> Istruisce gli incaricati al trattamento dei dati, fornendogli i compiti ed i limiti di accesso.

ANALISI DELLE COMPETENZE E FLUSSI INFORMATIVI

Nella nostra struttura i ruoli sono quelli riconducibili al seguente organigramma:

SOGGETTO	MANSIONE	LIMITI ACCESSO	NOTE
Titolare • Amaducci AnnaMaria • Forgiarini Alberto • Marcatelli Michele	Medico	Accede ai dati del proprio data base ed ai dati degli altri contitolari Amministra tutti i dati	Sensibili Economici e fiscali
Infermieri	Infermiere	Accede a tutti i dati dei titolari limitatamente ai propri compiti professionali	Sensibili Economici e fiscali In Corso di Copertura
Amministratore di rete e tecnici informatici • Marcatelli Michele	Manutenzione sistemi informatici	Accede ai dati limitatamente a quanto necessario ai fini della manutenzione	Sensibili solo in visione
Collaboratori • Bonavolontà Laura	Segreteria	Accettazione pazienti. Accede ai dati dei titolari Limitatamente ai compiti Esecutivi nei limiti impartiti	Sensibili Economici e fiscali

Medico sostituto • Seconi Marco	Medico	Accede ai dati del proprio data base ed ai dati degli altri contitolari Amministra tutti i dati	Sensibili Economici e fiscali e del personale e dei consulenti

TABELLA DEI TRATTAMENTI IN ATTO O POSSIBILI

INDIVIDUAZIONE TRATTAMENTO	TIPO DATI
Dati personali di Avvocati e professionisti cui vengono affidati incarichi o si rivolge per consulenze, quali quelli concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti a finalità fiscali o dati di natura bancaria	personali
Dati personali dei fornitori concernenti la reperibilità e la corrispondenza con gli stessi, nonché inerenti ai fini fiscali o dati di natura bancaria	personali
Dati personali degli assistiti e personali fornitori e/o clienti	personali
Dati personali del personale dipendente, quali quelli necessari al rapporto di lavoro, alla reperibilità ed alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali o dati di natura bancaria	personali
Dati sensibili del personale dipendente, conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assistenziali, o dati giudiziari del personale dipendente o l'adesione ad organizzazioni sindacali	sensibili
Dati sensibili degli assistiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare l'origine razziale ed etnica, le convinzioni o l'adesione ad organizzazioni a carattere religioso, politico, sindacale o filosofico	sensibili
Dati sensibili dei paziente, dagli stessi forniti o comunque acquisiti per l'espletamento idonei a rivelare lo stato di salute	sensibili
Dati sensibili di terzi, forniti dai pazienti o acquisiti per l'espletamento degli incarichi affidati allo studio, idonei a rivelare lo stato di salute	sensibili
Dati sensibili di clienti o terzi, comunque afferenti la vita sessuale	sensibili

MODALITA' DI RACCOLTA DEI DATI

I dati normalmente vengono raccolti

> Presso gli interessati

> Presso terzi (es. familiari del paziente)

> Presso altri professionisti sanitari e/o strutture sanitarie pubbliche o private

Metodi di elaborazione dati

> Con modalità informatizzate

PARTICOLARI FORME DI ELABORAZIONE

ELABORAZIONE	INTERCONNESSIONE	RESPONSABILE
Interconnessione con soggetti pubblici	Sistemi informativi regionali Progetto Sole in corso di attivazione	(Regione Emilia−Romagna) (in corso di copertura)

ACCESSO AI DATI E VALUTAZIONE DEI RISCHI

Alla base delle misure minime sono poste le modalità per l'accesso ai dati che devono avvenire solo da parte delle persone autorizzate ed esplicitamente incaricate. Ad esse dovranno essere assegnate o associate "credenziali di autenticazione", cioè parole chiave, codici identificativi, carte a microprocessore, token, certificati digitali, o dispositivi che riconoscano le caratteristiche biometriche. Tali credenziali dovranno consentire "l'autenticazione informatica" delle persone incaricate del trattamento di dati.

Inoltre, quando più persone incaricate accedono ai dati, è necessario associare ad ogni soggetto uno specifico profilo per l'accesso. Il profilo identifica i trattamenti dei dati che possono essere svolti e costituisce "l'ambito del trattamento consentito"; l'intero processo è definito "sistema di autorizzazione" per l'accesso ai trattamenti consentiti e preventivamente individuati.

La legge definisce anche i criteri con cui le credenziali devono essere scelte; ad esempio la parola chiave usata in un sistema di autenticazione deve essere 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 deve contenere riferimenti agevolmente riconducibili all'incaricato e deve essere 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 dovrà essere modificata almeno ogni tre mesi.

GESTIONE DEI SISTEMI INFORMATICI

Il corretto trattamento dei dati personali detenuti nel sistema informativo, richiede una corretta gestione dei sistemi. Al fine di meglio adempiere al compito si è ritenuto opportuno affidare a tecnici

specializzati la manutenzione dei sistemi. I soggetti incaricati sono i seguenti:

L'amministrazione delle password è stata affidata ai seguenti soggetti:

> Michele Marcatelli

MISURE DI SICUREZZA MINIME

Le misure minime di sicurezza richieste dalla legge sono tecniche, informatiche, organizzative, logistiche e procedurali e sono tutte orientate a ridurre i rischi che incombono sui dati personali trattati. Le misure da adottare per la protezione dei trattamenti elettronici dei dati sono sinteticamente elencate di seguito.

PROTEZIONE DA PROGRAMMI MALIGNI

PREVENZIONE DALLE VULNERABILITÀ, SALVATAGGIO DEI DATI

Alcune misure previste dal codice sono rivolte a tutelare la sicurezza di tutte le tipologie di dati personali dalle nuove emergenti criticità:

- i dati personali devono essere protetti contro il rischio di intrusione e dall'azione di virus, internet worm, programmi maligni, ecc., mediante l'attivazione di idonei strumenti elettronici, (ad esempio antivirus, firewall, ed altri adeguati sistemi) da tenere aggiornati;
- gli strumenti elettronici, nel caso di trattamenti di dati sensibili e giudiziari, devono essere aggiornati periodicamente con programmi che consentono di eliminare le vulnerabilità individuate e correggere i difetti del software individuati (patch, hot fix, service pack);
- i dati devono essere salvati su copie di riserva almeno settimanalmente nel rispetto di apposite disposizioni tecniche e organizzative.

BACKUP, SUPPORTI RIMOVIBILI, RIPRISTINO E DISASTER RECOVERY DEI DATI

I dati dovranno essere protetti da ulteriori misure di sicurezza, quali:

- strumenti elettronici che evitano gli accessi abusivi (intrusioni);
- procedure per la generazione e la custodia di copie di sicurezza dei dati (back up);
- 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;
- disposizioni per riutilizzare o distruggere i supporti rimovibili sui quali sono registrati tali dati;
- strumenti per il ripristino della disponibilità dei dati e dei sistemi entro tempi certi e compatibili con i diritti degli interessati, non superiori a sette giorni. Documento programmatico annuo sulla sicurezza.

LA CERTIFICAZIONE DELLE MISURE MINIME DI SICUREZZA

Le misure da adottare sono molte e potrebbe accadere che in azienda si preferisca avvalersi di installatori esterni, soprattutto nei casi in cui non si abbiano tutte le competenze necessarie. In tali circostanze, i titolari e/o l'amministratore del sistema devono farsi rilasciare dall'installatore una descrizione scritta dell'intervento effettuato. Il Codice, infatti, prevede questa circostanza e prescrive che chi adotta misure minime di sicurezza, avvalendosi di soggetti esterni alla propria struttura, riceve dall'installatore una descrizione scritta dell'intervento effettuato.

ANALISI DEI RISCHI

RISCHI DERIVANTI DA COMPORTAMENTI DEGLI OPERATORI		
Tipologia rischio	**livello**	**Contromisura**
sottrazione di credenziali di autenticazione	ALTO	immediata sostituzione password e denuncia autorità giudiziaria
carenza di consapevolezza, disattenzione o incuria	BASSO	Il personale è stato formato ed istruito
comportamenti sleali o fraudolenti	BASSO	Il personale è selezionato
errore materiale	BASSO	Il personale è formato

RISCHI DERIVANTI DA EVENTI RELATIVI AGLI STRUMENTI		
Tipologia rischio	**livello**	**Contromisura**
azione di virus informatici o di programmi suscettibili di recare danno	BASSO	Utilizzo idoneo software antivirus

spamming o tecniche di sabotaggio	BASSO	Utilizzo idoneo sistema firewall hardware integrato nel router di rete.
malfunzionamento, indisponibilità o degrado degli strumenti	BASSO	Idonea manutenzione
accessi esterni non autorizzati	BASSO	Idoneo sistema di sicurezza
intercettazione di informazioni in rete	BASSO	Idoneo sistema di sicurezza

RISCHI DERIVANTI DA EVENTI RELATIVI AL CONTESTO FISICO−AMBIENTALE		
Tipologia rischio	**livello**	**Contromisura**
ingressi non autorizzati a locali/aree ad accesso ristretto	BASSO	Idoneo sistema di sicurezza
sottrazione di strumenti contenenti dati	BASSO	Idoneo sistema di sicurezza e personale selezionato
eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti a incuria (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali)	BASSO	Idoneo sistema di sicurezza ed improbabilità dell'evento
guasto a sistemi complementari (impianto elettrico, climatizzazione)	BASSO	Sistema fornito di idoneo sistema di Back Up e di gruppo di continuità
errori umani nella gestione della sicurezza fisica	BASSO	formazione del personale

MONITORAGGIO DEL PROCESSO DI TRATTAMENTO

In occasione della revisione del documento programmatico della sicurezza, che dovrà essere effettuato entro il 30 Marzo di ogni anno, andranno verificate le seguenti circostanze e programmati gli interventi correttivi in relazione al progresso della tecnica ed ai rischi emersi nel corso dell'anno che in sede di prima analisi abbiamo così valutato

MISURA RICHIESTA	SOLUZIONE

Censimento e aggiornamenti dei trattamenti	Adottata
Lista degli incaricati	Adottata
Gestione delle credenziali di autenticazione	Adottata
Password personale, da rinnovarsi settimanalmente	Adottata
Protezione della sessione di lavoro	Adottata
Aggiornamento programmi per prevenire vulnerabilità e correggere difetti del software	Adottata
Adozione di misure idonee per assicurare l'integrità e disponibilità dei dati	Adottata
Salvataggio e ripristino dati	Adottata
Ripristino dei dati e sistemi salvati	Adottata
Difesa dagli accessi abusivi	Adottata
Protezione supporti rimovibili	Adottata
Analisi dei rischi informatici	Adottata
Formazione specifica degli incaricati	Adottata

DESCRIZIONE APPARATI E SISTEMI INFORMATICI IN USO

DESCRIZIONE	SISTEMA OPERATIVO	AGGIORNAMENTO	PROTEZIONI	UNITA'
server				0
pc collegati in rete (titolari + segretaria) ad architettura Intel 586 e superiori, con firewall hardware integrato nel router/modem, collegato ad Internet in banda larga, con antivirus	Windows su tutti i pc	aggiornamenti trimestrali del programma	antivirus aggiornato settimanalmente, firewall hardware integrato alla rete	4

PROTEZIONE INFORMATICA DEGLI STRUMENTI ELETTRONICI

SISTEMA DI AUTORIZZAZIONE

Il sistema di autorizzazione informatica utilizzato è: **Autorizzazione locale − con login/password –**

ALTRI SISTEMI DI PROTEZIONE OBBLIGATORI PER I DATI SENSIBILI

TRATTAMENTI DI DATI SENSIBILI	**PROTEZIONE SCELTA** (CIFRATURA / SEPARAZIONE)	**TECNICA ADOTTATA**	
		Descrizione	Informazioni utili
dati sensibili	cifratura	Vedi Documento allegato della società produttrice del programma gestionale Millewin	

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 (Regola 22 All. B “codice”).

CRITERI E PROCEDURE PER IL RIPRISTINO DELLA DISPONIBILITA’ DEI DATI

Appena terminate le operazioni, i supporti di back−up su cui sono memorizzati i dati vengono custoditi al fine di evitare accessi non autorizzati e trattamenti non consentiti (Regola 21 All. B “codice”).

BANCA/DATA BASE/ARCHIVIO DI DATI	**CRITERI E PROCEDURE PER IL SALVATAGGIO E IL**	**PIANIFICAZIONE DELLE PROVE DI RIPRISTINO**

	RIPRISTINO DEI DATI	
Dati personali degli assistiti e personali fornitori e/o clienti	esecuzione backup di sistema	

CRITERI E PROCEDURE PER IL SALVATAGGIO DEI DATI

BANCA DATI	CRITERI E PROCEDURE PER IL SALVATAGGIO	LUOGO DI CUSTODIA DELLE COPIE	STRUTTURA O PERSONA INCARICATA DEL SALVATAGGIO
Dati personali degli assistiti	Backup periodico su HD e Cd	Cassetti chiusi presso la sede principale	Responsabile del backup

DESCRIZIONE DEI LUOGHI E DEI SISTEMI DI PROTEZIONE

ARCHIVIO ELETTRONICO E CARTACEO

SISTEMI DI PROTEZIONE
Porte con chiave
Finestre protette
Cassetti con chiave

DESCRIZIONE DELLE ATTIVITA' DI FORMAZIONE

Gli argomenti oggetto di formazione per gli incaricati del trattamento dei dati riguardano (19.6 allegato B del codice):

- conoscenza dei rischi che incombono sui dati;
- misure disponibili di attività fisiche, logiche e informatiche per prevenire eventi dannosi;
- disciplina sulla protezione dei dati personali in rapporto alle relative attività;
- profili di responsabilità in merito al trattamento dei dati.

Interventi formativi programmati:

Periodo	Argomento	Relatore	Soggetto
Novembre 2005	Regole per la protezione dei dati nello Studio Medico	Marcatelli Michele	Tutti i membri della associazione e personale dipendente

Note: Nel corso dell'anno sono previste altre attività di formazione nel caso in cui vi siano cambiamenti di mansioni, o introduzione di nuovi significativi strumenti rilevanti ai fini del trattamento dei dati personali.

DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

Il titolare del trattamento dei dati deve stabilire i criteri da adottare per garantire l'adozione delle misure minime di sicurezza nel caso in cui il trattamento dei dati personali venga affidato all'esterno della struttura (19.7 allegato B codice). Ad esempio, sarebbe opportuno prevedere che il trasporto di fascicoli o files dall'azienda al domicilio di un collaboratore / professionista / dipendente fosse subordinato all'adozione da parte di questi soggetti di particolari misure di sicurezza fisiche e telematiche (custodia accurata del fascicolo cartaceo, cifratura dei dati elettronici). Per quanto riguarda, invece, l'affidamento presso soggetti terzi, il titolare è tenuto a descrivere l'attività che è stata delegata e quali tipi di dati in essa vengono trattati. Per ogni operazione o gruppo di operazioni su dati personali, effettuati all'esterno della struttura, sarebbe consigliabile creare un'apposita modulistica.

TRATTAMENTI AFFIDATI ALL'ESTERNO

Soggetto esterno	Trattamenti di dati interessati	modalità affidamento	Descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Consulente responsabile del servizio protezione e prevenzione	Accede ai dati relativi all'incarico affidato (Sensibili nei limiti della sicurezza del personale)	cartaceo / informatico	Richiesta certificazione di conformità (D. Lgs. 196/2003)
Consulente legale	Accede ai dati anche sensibili limitatamente al caso affidato	cartaceo / informatico	Richiesta certificazione di conformità (D. Lgs. 196/2003)

Consulente del lavoro	Accede ai dati economici, fiscali e del personale e dei consulenti (Sensibili limitatamente al personale ed anagrafiche)	cartaceo / informatico	Richiesta certificazione di conformità (D. Lgs. 196/2003)
Consulente Commercialista	Dati economici, ed economici compresi quelli dei consulenti (Sensibili limitatamente alle anagrafiche)	cartaceo / informatico	Richiesta certificazione di conformità (D. Lgs. 196/2003)

SCHEMA DELLE PASSWORD

Gruppo	Generalità	Nome utente	Password	Data
TITOLARI	AnnaMaria Amaducci			
TITOLARI	Alberto Forgiarini			
TITOLARI	Michele Marcatelli			
SOGGETTI	Michele Marcatelli			
SOGGETTI	Marco Seconi			
SOGGETTI	Laura Bonavolontà			