ASL SALERNO
AZIENDA SANITARIA LOCALE SALERNO

PRIVACY - DPS

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DATI PERSONALI E SENSIBILI

Azienda Sanitaria Locale Salerno

Redatto in conformità alla norma

DLGS 196/2003

ASL SALERNO
AZIENDA SANITARIA LOCALE SALERNO

PRIVACY - DPS

Elenco distribuzione ed approvazioni:

Copia n°	Destinatario
1	Azienda Sanitaria Locale Salerno

Approvazione

		Titolare del trattamento
Firma		

Data ultima revisione

	REVISIONI		
Riferimenti	Descrizione aggiornamento	Verifica	Approvazione

ASL SALERNO
AZIENDA SANITARIA LOCALE SALERNO

PRIVACY - DPS

SEZIONE 0. INTRODUZIONE

Lo scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare presso l'Azienda Sanitaria Locale Salerno (d'ora innanzi denominata Azienda), affinché siano rispettati gli obblighi, in materia di sicurezza, previsti dal Decreto Legislativo 196/2003 detto "Codice in materia di protezione dei dati personali", e dal Disciplinare Tecnico in materia di misure minime di sicurezza contenente norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali (Allegato B del D. Lgs. 196/2003).

Il presente Documento Programmatico sulla Sicurezza dei Dati Personali (DPS) deve essere divulgato a tutti i membri dell' Azienda coinvolti nella gestione dei dati. Tutti i membri dell' Azienda coinvolti nella gestione dei dati devono rispettare le prescrizioni in esso contenute ed operare, nell'ambito della propria organizzazione, in modo da:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi cartacei contenenti dati personali comuni o sensibili;
- minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali;
- minimizzare la probabilità che i trattamenti dei dati personali siano modificati senza autorizzazione

0.1 Campo di applicazione del Documento Programmatico sulla Sicurezza

II presente Documento Programmatico sulla Sicurezza dell' Azienda Sanitaria Locale Salerno si applica a qualsiasi trattamento di dati personali e in particolare dati sensibili, effettuato da membri dell' Azienda, o da terzi, per conto dell' Azienda Sanitaria Locale Salerno.

SEZIONE 1. PRESENTAZIONE DELL' AZIENDA SANITARIA LOCALE SALERNO.

L' Azienda Sanitaria Locale Salerno ha sede legale in via Nizza n. 146, 84124 Salerno.

L'Azienda ha per Scopi:

1) **Assistenza Sanitaria e Sociale**

Sono Organi della Azienda:

- **Commissario straordinario: Maurizio Bortoletti**
- **Strutture generali**
- **Distretti sanitari**
- **Presidi ospedalieri**

Dati della Azienda:

- **Ragione Sociale : Azienda Sanitaria Locale Salerno.**
- **Commissario straordinario: Maurizio Bortoletti**
- **Sede Legale : Via Nizza n. 146 Salerno, 84124 Salerno**

SEZIONE 2. PRESENTAZIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (DPS)

Ai sensi del Disciplinare Tecnico in materia di misure minime di sicurezza, entro il 31 marzo di ogni anno, il Titolare di un trattamento di dati sensibili o di dati giudiziari è tenuto a redigere, anche attraverso il Responsabile del trattamento, se designato, un Documento Programmatico sulla Sicurezza dei dati contenente idonee informazioni riguardo:

1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al punto 23 del Disciplinare;
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 più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione deve essere programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
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 conformità al codice, all'esterno della struttura del titolare;
8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24 del Disciplinare, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

2.1 Struttura del DPS

Questo DPS è suddiviso in Sezioni numerate.

2.2 Revisioni

Questo Documento Programmatico sulla Sicurezza:

- **È stato verificato e redatto dal Titolare del trattamento**

I Responsabili del trattamento sono gli unici soggetti autorizzati ad apportare modifiche o aggiornamenti al presente documento, da sottoporre all'approvazione del Titolare.

La gestione del DPS, e quindi gli ampliamenti, le revisioni e le modifiche sono di esclusiva competenza dei Responsabili del Trattamento, che hanno anche la responsabilità della distribuzione del documento del documento stesso.

Qualora il DPS, con la revisione, subisca modifiche sostanziali e profonde si dovrà provvedere alla emissione di una nuova edizione dello stesso.

Se il totale delle revisioni dovesse superare il numero di 10 per edizione si dovrà provvedere all'emissione di una nuova edizione.

Ogni qual volta si presenti necessaria l'emissione di una nuova edizione, si provvederà a:

- **ritirare tutte le copie controllate già distribuite e distruggerle;**
- **aggiornare la lista di distribuzione;**
- **distribuire la copia aggiornata.**

2.3 Aggiornamento

II presente Documento Programmatico sulla Sicurezza dei dati deve essere aggiornato entro il 31 marzo di ogni anno, ai sensi del Disciplinare Tecnico in materia di misure minime di sicurezza (allegato B del D. Lgs. 196/2003).

In sede di aggiornamento, il Titolare, coadiuvato dai Responsabili, esamina tutte le informazioni derivanti dalle attività di controllo effettuate. È chiamato quindi a valutare la validità delle misure adottate e la corretta applicazione da parte degli incaricati.

Inoltre dovrà valutare la necessità dell'Azienda di effettuare nuovi tipi di trattamenti o di trattare una nuova tipologia di dati. Quindi dovrà aggiornare l'analisi dei rischi e predisporre misure minime di sicurezza idonee, e provvedere ad eventuale nuova notificazione al Garante.

SEZIONE 3. GLOSSARIO

***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.**

***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.**

***DATI IDENTIFICATIVI*: i dati personali che permettono l'identificazione diretta dell'interessato.**

***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, filosofia), politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.**

***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.**

***TITOLARE DEL TRATTAMENTO*: 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.**

***RESPONSABILE DEL TRATTAMENTO*: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.**

***INCARICATI DEL TRATTAMENTO*: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.**

***INTERESSATO*: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.**

***BANCA DI DATI*: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.**

***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 del D. Lgs. 196/03.**

***STRUMENTI ELETTRONICI*: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.**

***AUTENTICAZIONE INFORMATICA*: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.**

***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.**

***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.**

SEZIONE 4. DOCUMENTAZIONE

L'applicazione del "Codice in materia di protezione dei dati personali" contempla l'applicazione, oltre che del presente DPS, anche dei seguenti tipi di documenti:

- **Procedure,**
- **Istruzioni operative,**
- **Documenti di registrazione,**
- **Documenti di origine esterna.**

4.1 Procedure

Le Procedure sono documenti primari, anche di carattere interfunzionale, che disciplinano e coordinano le attività, definiscono modalità operative, documentazione, risorse e responsabilità al fine di garantire la sicurezza dei dati trattati.

4.2 Istruzioni operative

Le istruzioni operative sono disposizioni scritte che specificano o descrivono le modalità esecutive ed i riferimenti per svolgere un particolare trattamento, al fine di garantire la sicurezza nella gestione dei dati all'interno dell'Azienda Sanitaria .

4.3 Documenti di Registrazione

Sono documenti utilizzati per la registrazione di precise attività, talvolta regolamentate da Procedure, quali controllo e verifica, formazione, lettera di nomina dei responsabili, e rappresentano la dimostrazione oggettiva e documentata della loro applicazione.

4.4 Documenti di origine esterna

Sono documenti acquisiti dall'Azienda Sanitaria Locale Salerno.

4.5 Sistema Informativo

L' Azienda Sanitaria Locale Salerno utilizza un sistema informativo costituito da PC, che hanno accesso alla rete Internet. I PC sono muniti di: antivirus (periodicamente aggiornato); firewall; proxy server. Pertanto il sistema è in grado di garantire una corretta, efficiente e sicura gestione dei dati, delle informazioni e dei documenti.

Gli archivi del sistema informativo sono progettati e realizzati con lo scopo di garantire:

- **Riservatezza dei dati relativi ai soggetti attivi del Percorso Privacy, tramite la regolamentazione degli accessi; ad ogni archivio, infatti, sono associate le relative regole di accesso, utilizzo e condivisione da parte dei membri dell'organizzazione.**

Sicurezza dei dati dei soggetti attivi del Percorso Privacy, il sistema informativo è in grado di garantire la sicurezza e l'integrità di tutti i dati e le informazioni relative ai sopra citati soggetti tramite: o procedure di back-up di tutti gli archivi al fine di garantire il recupero delle informazioni anche in caso di malfunzionamenti del sistema informativo, o livelli di protezione (password) per gli accessi alla rete informativa, o strumenti di intercettazione ed eliminazione dei virus elettronici.

SEZIONE 5. IMPEGNO DEL TITOLARE

L' Azienda Sanitaria Locale in funzione delle proprie attività di lavoro e dello scopo del presente DPS:

- **assicura la disponibilità di risorse economiche, tecnologiche, organizzative ed umane secondo le modalità espresse alle sezioni 7 e 8;**
- **emette la seguente Dichiarazione di Impegni.**

Impegno del Titolare del trattamento

Per la particolarità delle attività svolte, l' Azienda Sanitaria Locale Salerno si è sempre posta il problema di garantire la riservatezza e l'integrità dei dati relativi ai propri stakeholders.

Gli sforzi compiuti e l'esperienza accumulata hanno permesso di realizzare accorgimenti tali da perfezionare la gestione dei dati personali e/o sensibili.

Pertanto il Titolare del trattamento concorda pienamente con le disposizioni del Codice in materia di protezione dei dati personali, scorgendo in esso oltre all'obbligo di uniformarsi, la possibilità di migliorare ulteriormente il proprio sistema di gestione dati al fine di renderlo ancora più efficiente. La sicurezza nella gestione dei dati personali, e in particolare di quelli sensibili, deve essere adeguata, e verificata. Tutti i soggetti attivi del Percorso Privacy dell' Azienda Sanitaria Locale Salerno saranno pertanto sensibilizzati al fine di ottenere un ambiente sano e sicuro per ciò che attiene la gestione dei dati. La realizzazione di un Documento Programmatico sulla Sicurezza dei dati, voluto dal Decreto Legislativo 196/03, offre la possibilità di formalizzare e quindi di mettere a conoscenza tutti gli stakeholders delle misure di sicurezza adottate e da applicare.

Il Titolare del trattamento è sempre tenuto informato dei problemi riguardanti la sicurezza dei dati, e garantisce la più completa indipendenza ed autonomia al Responsabile del Trattamento, delegandogli la responsabilità di tale sicurezza.

SEZIONE 6. RESPONSABILITÀ E AUTORITÀ

II Titolare del trattamento dell' Azienda Sanitaria Locale Salerno ha definito le responsabilità, l'autorità ed i rapporti reciproci dei Soggetti attivi del Percorso Privacy per:

- **implementare le misure minime di sicurezza individuate a seguito dell'analisi dei rischi;**
- **identificare e registrare ogni problema relativo alla sicurezza nel trattamento dei dati;**
- **verificare l'efficacia delle soluzioni adottate;**
- **gestire eventuali problemi fino all'adozione di misure di sicurezza più idonee.**

Ciò allo scopo di stabilire i rapporti reciproci che devono avere la libertà organizzativa e l'autorità necessaria a:

- **identificare e registrare ogni problema relativo alla sicurezza nel trattamento dei dati;**
- **avviare, proporre e fornire eventuali soluzioni attraverso i canali stabiliti;**
- **verificare l'attuazione delle soluzioni.**

A tale scopo l' Azienda Sanitaria Locale Salerno ha definito:

- **i Mansionari.**

6.1 Titolare del Trattamento

II Titolare del trattamento è la figura individuata nell'art. 28 del D. Lgs. 196/03, ed è suo compito:

- **esercitare potere decisionale sulle finalità e sulle modalità del trattamento dei dati personali;**
- **designare il responsabile del trattamento e specificarne per iscritto i compiti;**
- **vigilare sul rispetto, da parte del Responsabile del trattamento, delle proprie istruzioni, nonché sull'osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza, anche tramite apposite verifiche e controlli periodici.**

Il Titolare del trattamento è l'Azienda Sanitaria Locale Salerno.

6.2 Responsabile del trattamento

II Responsabile del trattamento è nominato dal Titolare del trattamento ai sensi dell'art. 29 del D. Lgs. 196/03, individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Essi:

- **vigilano sulla sicurezza dei dati personali comuni e sensibili comunque gestiti (automatizzati e non) garantendo che l'Azienda sia dotata di adeguate misure organizzative, procedurali e tecniche per minimizzare i rischi cui sono soggetti i dati personali di cui l' Azienda è titolare;**
- **redigono il DPS e ne curano le successive modifiche/revisioni/aggiornamenti;**

- effettuano periodici controlli e verifiche in merito al rispetto delle prescrizioni contenute nel presente DPS e promuovono l'aggiornamento dello stesso sulla base di eventuali mutamenti organizzativi e tecnologici;
- promuovono lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel DPS;
- promuovono annualmente la valutazione del livello di rischio cui sono esposti i dati personali, ed aggiornano il relativo documento;
- informano il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti di sicurezza;
- promuovono lo svolgimento di un adeguato programma di addestramento degli Incaricati del trattamento e mantengono attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;
- forniscono guida e supporto agli Incaricati del trattamento in merito alla sicurezza.

Tali soggetti sono identificati nelle persone di tutti i Dirigenti di Struttura Complessa e di Dipartimento.

6.3 Incaricati del trattamento

Gli Incaricati del trattamento sono gli addetti al trattamento dei dati individuati ai sensi dell'art. 30 del D. Lgs. 196/03; essi:

- devono attenersi, per i trattamenti di competenza, alle prescrizioni, alle procedure operative contenute nel DPS e alle direttive del Responsabile del trattamento;
- devono rispettare le norme di sicurezza per la protezione dei dati personali;
- non possono modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del trattamento.

Gli Incaricati al trattamento all'interno dell' Azienda Sanitaria Locale Salerno sono individuati in base al tipo di dati che trattano, e la formalizzazione dell'incarico avverrà secondo il criterio delle classi omogenee di appartenenza del personale dipendente, suddiviso per qualifica e mansione

Per il mansionario degli incaricati si rimanda all'allegato: "istruzione incaricati".

6.4 Amministratore di sistema

È suo compito:

- **sovrintendere alle risorse dei sistemi operativi degli elaboratori e dei sistemi delle basi dati per consentirne l'utilizzazione;**
- **sviluppare, realizzare e mantenere aggiornate, per le banche dati personali gestite con sistemi informatici, le misure di sicurezza, in accordo con le norme e le procedure operative contenute nel DPS;**
- **monitorare, se richiesto, i piani di adeguamento alla sicurezza;**
- **fornire guida e supporto agli Incaricati del trattamento;**
- **effettuare periodici controlli e verifiche tecniche in merito al rispetto delle prescrizioni contenute nel DPS;**
- **amministrare e gestire la sicurezza informatica operando, se necessario, anche come gestore delle password;**
- **amministrare la sicurezza mantenendo aggiornati gli User ID ed i profili di accesso ai sistemi, alle applicazioni ed alle banche dati secondo le esplicite autorizzazioni ricevute;**
- **mantenere una traccia di audit di tutte le operazioni effettuate.**

L'Amministratori di Sistema è individuato nella persone del Direttore dell' U. O. C. Sistemi Informativi - Dott. Gianni Vito, dirigente CED - quale Amministratore di Sistema in House. Si rimanda al contratto di natura privatistica, stipulato con l'Azienda Sanitaria Locale Salerno.

La nomina formale verrà ulteriormente rettificata secondo il modello specifico allegato al presente Documento (Allegato 13 - Nomina Amministratore Di Sistema).

SEZIONE 7. RISORSE UMANE

Nell'ambito della gestione dei dati personali la centralità dell'opera dell'uomo è indispensabile per l'efficacia dell'attuazione delle misure minime di sicurezza.

I membri dell' Azienda coinvolti nella gestione dei dati vanno quindi forniti del giusto grado di sensibilizzazione e di conoscenza necessario per una corretta applicazione del presente Documento Programmatico sulla Sicurezza, nonché per il suo continuo adeguamento. La Formazione porta alla consapevolezza della necessità di cambiamenti e fornisce gli elementi per poter realizzare cambiamenti e sviluppi.

La Formazione costituisce un elemento fondamentale per il miglioramento della gestione dei dati. Allo scopo di garantire soprattutto l'efficacia delle misure minime di sicurezza stabilite, è compito del Titolare del trattamento individuare e assegnare le responsabilità coinvolte.

Premesso che tutti i membri dell'Azienda coinvolti nella gestione dei dati devono essere adeguatamente formati sulla necessità di stabilire e rispettare delle misure minime di sicurezza per il trattamento di dati personali, particolare attenzione è volta alla sensibilizzazione e formazione degli Incaricati del trattamento.

7.1 Pianificazione ed esecuzione delle attività di formazione

Il Sistema Sanitario moderno, al fine di poter rispondere in modo adeguato ed efficiente alle domande di salute dei cittadini, deve poter disporre e trattare tutti i dati necessari. L'uso delle informazioni non deve sconfinare, tuttavia, nell'abuso da parte delle strutture sanitarie e degli operatori ad esse afferenti; a questo scopo va prestata particolare attenzione alla difesa della privacy.

Il Codice in materia di protezione dei dati personali, introdotto nell'ordinamento con il decreto legislativo 196/03, onde proteggere da intrusioni o azioni illegittime il patrimonio informativo individuale di ciascuna persona, pone, in capo agli organismi sanitari, una serie di obblighi.

Ne consegue che gli operatori della sanità hanno il dovere, ma prima ancora, il diritto di conoscere in maniera dettagliata ed esaustiva le diverse modalità di applicazione e le procedure da seguire. Il Legislatore raccomanda, infatti, che i dipendenti, sin dal momento dell'ingresso in servizio o in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, che abbiano rilevanza rispetto al trattamento di dati personali, siano messi nella condizione di poter adempiere a tali obblighi mediante formazione iniziale e in itinere (regola 19.6,Allegato B Codice Privacy).

La formazione e l'informazione di tutto il personale acquistano, pertanto, una funzione assolutamente determinante allo scopo di promuovere la sensibilizzazione sul problema della tutela della privacy e di favorire l'assunzione, nell'ambito dell'organizzazione, di atteggiamenti e comportamenti coerenti con quanto sancito dalla normativa, per il miglioramento dell'assistenza al paziente ed alla famiglia.

Il presente Progetto formativo persegue tali Finalità:

- Sensibilizzazione del personale e promozione della cultura della privacy
- Assicurare un elevato livello di tutela dei diritti , delle libertà fondamentali e della dignità degli interessati
- Conoscenza della normativa vigente in materia di riservatezza dei dati

- Interiorizzazione del valore professionale ed umano della difesa della privacy in sanità

Obiettivi generali:

Il progetto intende favorire nei partecipanti il trasferimento nella specifica quotidianità lavorativa dei contenuti appresi sul piano del *sapere*, del *saper fare* e del *saper essere*, attraverso l'assunzione di atteggiamenti, l'acquisizione di comportamenti, l'utilizzo di conoscenze che confluiscano nella capacità di gestire adeguatamente, sia in forma cartacea che elettronica, le informazioni riguardanti l'utenza interna ed esterna.

Obiettivi specifici:

A breve termine

- Motivare il personale al problema della difesa della privacy
- Adempiere agli obblighi sanciti dal DLgs 196/03
- Standardizzare le procedure e prevenire i comportamenti illeciti

A medio termine

- Favorire processi di comunicazione efficaci attraverso la corretta gestione delle informazioni
- Assumere la policy aziendale sull'utilizzo dei dati come un indicatore di qualità delle cure
- Ridurre lo stato di disagio cui sono sottoposti i pazienti e le famiglie

Articolazione e destinatari del progetto

Il progetto formativo è rivolto a tutto il personale dell'Azienda Sanitaria Locale Salerno ed è articolato in due percorsi diversificati in base al target:

1. Responsabili del trattamento dei dati
2. Incaricati al trattamento dei dati

Entrambi i percorsi prevedono tre fasi:

1. Modulo di base
2. Modulo di approfondimento
3. Attività di audit

Materiale didattico e informativo

E' prevista la fornitura di materiale didattico ed informativo anche attraverso la distribuzione di linee guida aziendali, di opuscoli informativi, cd, news letter.

Metodo

La metodologia prevede un approccio a didattica mista con lezioni frontali di tipo interattivo accompagnate da esercitazioni al fine di fornire stimoli e spunti per la riflessione ed il confronto, favorendo operazioni di problem – solving, attraverso processi di autovalutazione, per l'acquisizione di competenze in tema di tutela della privacy.

I Corso di formazione per i Responsabili del trattamento

Il primo percorso si rivolge alle figure apicali nominate Responsabili del trattamento dal Titolare ed è articolato in due moduli di 8 ore ciascuno

1° modulo

1^ sessione: 4 ore di lezione frontale caratterizzata da un approccio interattivo

Programma

Introduzione al Testo Unico per la protezione dei dati personali

Disposizioni generali sul trattamento dei dati. Concetti fondamentali

La protezione dei dati personali: finalità, necessità, oggetto, soggetti, operazioni

Le modalità di trattamento dei dati personali

Il trattamento dei dati in ambito sanitario

L'informativa all'interessato ed il consenso

Gli adempimenti

La notificazione del trattamento

Obblighi di comunicazione al Garante

Autorizzazioni

Misure e obblighi di sicurezza

La disciplina giuridica del trattamento dei dati personali

Tutela dell'interessato, responsabilità e sanzioni

2^ sessione: 4 ore di lezione con metodologia teorico - pratica articolata in esercitazioni e simulazioni con lavori di gruppo - Conclusioni operative

2° modulo

Giornata di studio

A completamento del percorso formativo sarà organizzata una Giornata di studio al fine di di dar modo ai corsisti di approfondire e di consolidare gli argomenti trattati nel precedente incontro. L'evento, da realizzare, eventualmente, in raccordo con i rappresentanti di Istituzioni autorevoli quali il Garante per la Protezione dei Dati Personali ed esperti in materia di tutela della privacy e di gestione informatica dei dati,

sarà volto alla promozione del dialogo interaziendale ed interistituzionale, al fine di favorire un approccio proattivo alla materia, permettendo così di cogliere la legge quale strumento di tutela e garanzia per il cittadino – utente.

Il rispetto alla riservatezza, dunque, non viene inteso quale mero adempimento alla normativa ma ulteriore fattore di qualità per quanti operano quotidianamente nel settore sanitario e, pertanto, sono portati a confrontarsi con problemi connessi alla gestione dei rischi e all'adozione di idonee misure di sicurezza.

II Corso di formazione per incaricati del trattamento.

Nella fase iniziale, al fine di poter assicurare l'aggiornamento a tutto il personale incaricato al trattamento dei dati ed afferente ad ogni singola struttura, dislocata nelle diverse sedi aziendali, risulta opportuno attivare un percorso di formazione - informazione di 6 ore di tipo frontale, volto alla sensibilizzazione del personale alla materia.

Obiettivi del corso:

Prevenire diffusioni improprie di notizie "a terzi non legittimati" ed introdurre, nello stesso tempo, regole di condotta e modalità operative, miranti a salvaguardare il patrimonio informativo dell'Azienda, i cui dati personali, identificativi e sensibili degli utenti, interni ed esterni, costituiscono una componente importante ed essenziale.

Articolazione dei moduli:

Le attività formative per gli incaricati partiranno dall'impianto normativo e dai concetti fondamentali prescritti dal Codice per poi proseguire con lezioni di taglio pratico durante le quali verrà illustrato il Regolamento aziendale, saranno letti e commentati i

Provvedimenti e le Pronunce del Garante prescritti agli organismi sanitari, si discuterà sulle parti salienti del Documento Programmatico della Sicurezza.

Fasi:

1. modulo di base di n. 6 ore con lezioni di tipo frontale

PROGRAMMA

Principi generali DLgs 196/03 (finalità, definizioni, oggetto ed ambito di applicazione)

Diritti dell'interessato: Informativa e consenso al trattamento, diritto di accesso ai dati personali, riscontro all'interessato

Identificazione delle responsabilità e ripartizione dei compiti

L'organigramma privacy: Titolare - Responsabili - Incaricati

Istruzioni e procedure: aspetti teorici e aspetti operativi

Il Documento Programmatico sulla Sicurezza: obblighi e adempimenti

La trasparenza, la responsabilità, la sicurezza nel trattamento dei dati personali con l'ausilio di mezzi elettronici o cartacei

Analisi, conoscenza e valutazione dell'organizzazione e dei trattamenti

Strumenti e fattori di rischio cui sono soggetti i dati

Misure di sicurezza per l'integrità e la disponibilità dei dati

2. modulo di n. 4 ore con laboratori di approfondimento volti all'analisi di casi reali ed alla risoluzione di problemi mediante esercitazioni e simulazioni riguardanti la

specificità dei ruoli e delle responsabilità ricoperti, delle mansioni svolte e delle esigenze operative da affrontare.

3. La terza fase del progetto prevede, per entrambi i percorsi formativi, attività di audit con la finalità di migliorare la qualità e la sicurezza nella gestione dei trattamenti dati. A sei mesi di distanza dal corso di formazione verranno effettuate, in raccordo con i responsabili dei trattamenti, verifiche sistematiche e strutturate sugli esiti dei processi organizzativi messi in atto nelle diverse macroarticolazioni, finalizzate alla risoluzione di eventuali criticità.

7.3 Motivazione e consapevolezza dei soggetti attivi dell'Azienda

I membri dell' Azienda coinvolti nella gestione dei dati vengono motivati attraverso azioni di informazione sugli scopi del progetto, sollecitando un comportamento attivo da parte di tutti nella ricerca delle misure di miglioramento. In particolare essi saranno opportunamente coinvolti nella ricerca delle cause a monte che hanno generato le non conformità durante le attività di gestione dei dati, raccogliendo nelle dovute forme i suggerimenti sulle azioni correttive da intraprendere.

Tutti i membri dell' Azienda coinvolti nella gestione dei dati vengono edotti sul "Codice in materia di protezione dei dati personali", al fine di trasmettere loro l'importanza del lavoro dei singoli in conformità col Codice stesso.

In particolare, è previsto inizialmente lo svolgimento di giornate di formazione nella quale saranno sensibilizzati i membri dell'Azienda coinvolti nella gestione dei dati sui rischi generati dalla gestione dei dati personali e sugli interventi correttivi adottati; altri eventi formativi saranno programmati, all'occorrenza, in sede di audit del Sistema

di gestione della Privacy o in base a specifiche esigenze rilevate dai Responsabili del Trattamento.

Disposizioni circa le responsabilità relative alla gestione dei dati, nel rispetto del DLgs 196/03, sono state previste nei mansionari, consegnati ad ogni membro del Percorso attivo (sia responsabile che incaricato del trattamento) dell'Azienda coinvolto nella gestione dei dati.

SEZIONE 8. INFRASTRUTTURE

I mezzi, le attrezzature, i sistemi elettronici, gli archivi e tutto quanto altro occorre alla esecuzione delle attività di gestione dei dati, il loro stato di efficienza, la loro adeguatezza alle attività associative sono elementi essenziali per il corretto espletamento delle suddette attività nel rispetto del Codice di trattamento dei dati personali.

8.1. identificazione delle risorse da proteggere

Le risorse coinvolte nel trattamento dei dati personali sono state suddivise in alcune categorie:

- luoghi fisici: **Sono stati analizzati tutti i luoghi ove fisicamente si svolge il trattamento dei dati, si trovano i sistemi e gli strumenti (o apparecchiature elettroniche) di elaborazione e di telecomunicazione e i luoghi ove si conservano i dati.**

- Risorse hardware: **Sono state analizzate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento. Tra queste particolare rilievo hanno: i server del Sistema Informativo Informatico dell'Azienda, ove sono conservati i dati in formato elettronico, e su cui vengono eseguiti i programmi che elaborano/eseguono i trattamenti dati. Inoltre sono state analizzate le attrezzature e le strutture dedicate alle telecomunicazioni. Rientrano in questa categoria tutte le cpu; i terminali; i pc; le stampanti; i server; gli apparati attivi di rete; le linee di comunicazione; ecc…**

- Risorse dati: **Sono stati analizzati tutti gli archivi contenenti dati personali e sensibili trattati dall'Azienda, con particolare riferimento a quelli in formato elettronico/informatico.**

- Risorse Software e supporti di memorizzazione: **Sono stati analizzati i Sistemi Operativi ed i software applicativi mediante i quali vengono gestiti i server e gli elaboratori aziendali ed effettuati i trattamenti automatizzati. Rientrano in questa categoria i sistemi operativi; i software di base (utilità, diagnostici, ecc…) ; i software applicativi; i gestori di basi di dati; i software di rete; tutti i programmi in formato sorgente ed oggetto.**

SEZIONE 9. ANALISI DEI RISCHI

L' Analisi dei Rischi risponde alla prescrizione introdotta dal Disciplinare tecnico in materia di misure minime di sicurezza, che impone alle Aziende titolari di trattamenti di dati personali di redigere, entro il 31 marzo di ogni anno, un documento programmatico sulla sicurezza dei dati.

Secondo le security practices validate a livello internazionale, la corretta gestione della sicurezza presuppone una metodologia di processo o ciclo continuo, in cui la "analisi dei rischi" innesca l'intero processo di gestione della sicurezza. Le fasi concatenate in cui il ciclo è suddiviso sono:

- **analisi dei rischi;**
- **politiche di sicurezza;**
- **piano di attuazione;**
- **amministrazione della sicurezza;**
- **audit e test;**

per tornare poi nuovamente all'analisi dei rischi, ed innescare così il ciclo continuo.

L' analisi dei rischi predisposta dall'Azienda , ed esposta nel relativo documento PRIVACY - Analisi dei Rischi - , rappresenta lo strumento fondamentale per la predisposizione del DPS stesso, nonché lo strumento di controllo dell'intero sistema sicurezza dell'Azienda. L'analisi dei rischi effettuata ha evidenziato una sostanziale aderenza delle misure di sicurezza adottate dall'Azienda con quanto disposto dalla normativa vigente. Le principali carenze evidenziate sono state colmate con interventi di carattere organizzativo/procedurale.

Si rimanda pertanto a tale documento per una esposizione dettagliata dell'analisi dei rischi effettuata presso l' Azienda e sulle conseguenti misure di prevenzione adottate; nella sezione successiva viene descritto il modello che l' Azienda ha deciso di adottare per la gestione della sicurezza dei dati personali di cui è titolare.

SEZIONE 10. PRESCRIZIONI DI SICUREZZA

In questa sezione sono definite le regole fondamentali che l' Azienda ha adottato per la realizzazione delle misure di sicurezza fisiche, logiche ed organizzative, nella gestione dei dati personali e dei dati sensibili oggetto di trattamento.

Il rispetto delle prescrizioni contenute all'interno del DPS è obbligatorio e oggetto di verifica e audit, eccezion fatta per i sistemi isolati (non in rete) che non contengono dati personali.

Il documento elenca le contromisure di natura fisica, logica ed organizzativa da adottare al fine di ridurre i rischi individuati. Le misure sono suddivise in :

- **Misure di mantenimento: da controllare ed attivare per le nuove installazioni e per i nuovi progetti**
- **Misure aggiuntive: che perfezionano la sicurezza del Sistema Informativo.**

10.1. misure di sicurezza di tipo fisico di mantenimento

DESCRIZIONE MISURA	NOTE ED INDICAZIONI PER LA CORRETTA APPLICAZIONE
SF1 – Sala macchine	Le sale macchine vanno chiuse a chiave a meno che non siano fisicamente presidiate. Una copia delle chiavi va depositata in portineria o altro luogo definito, accessibile solo al personale autorizzato. Le chiavi vanno opportunamente gestite, in modo che vengano in possesso solo delle persone incaricate e che non vi siano blocchi dei servizi erogati.
SF2 – Locali che ospitano Sistemi di rete o telefonici	I locali che ospitano Sistemi di Rete o Telefonici vanno chiusi a chiave a meno che non siano fisicamente presidiati. Le chiavi vanno opportunamente gestite in modo che vengano in possesso solo delle persone autorizzate e che non vi siano blocchi dei servizi erogati.
SF3 – Locali che ospitano Computer contenenti Banche dati non centralizzate	Tali locali vanno chiusi a chiave a meno che non siano fisicamente presidiati. Le chiavi vanno opportunamente gestite in modo che vengano in possesso solo delle persone autorizzate e che non vi siano blocchi dei servizi erogati.
SF4 – Armadi di rete	Gli armadi di rete vanno chiusi mediante apposita chiave. Una copia della chiave va depositata presso il Servizio per l'Informatica ed una copia presso l'Ufficio Tecnico.
SF5 – Custodia di archivi cartacei	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 o documenti sono custoditi dagli incaricati in modo che ad essi non accedano persone prive di autorizzazione. L'accesso agli archivi contenenti dati sensibili o giudiziari va controllato; le persone che vi accedono sono preventivamente autorizzate.

SF6 – Custodia di supporti magnetici	I supporti ausiliari di memorizzazione (dischetti o altro) utilizzati per le attività di backup o di salvataggio o per la memorizzazione temporanea o per la conservazione dei dati trasmessi all'azienda da strutture pubbliche esterne, vanno conservati in locali distinti da quelli ove risiedono gli elaboratori che contengono gli stessi dati, in contenitori chiusi a chiave. Le chiavi vanno opportunamente gestite in modo che vengano in possesso solo delle persone autorizzate e che non vi siano blocchi dei servizi erogati.
SF7 – Dispositivi Antincendio	Nei locali delle sale macchine o nelle immediate vicinanze saranno disponibili estintori o altri strumenti antincendio.
SF8 – Ridondanza e continuità di alimentazione elettrica	I server sanitari ed amministrativi vanno installati nelle sale macchine ed alimentati almeno attraverso gruppo di continuità statica o preferibilmente gruppo elettrogeno e gruppo di continuità statica. Nel caso di interruzioni di energia elettrica dovuta a motivi di forza maggiore, sarà attivata una procedura congiunta di azione tra Ufficio Tecnico e Servizio per l'Informatica, in modo da garantire il corretto spegnimento dei database e delle macchine. L'alimentazione delle macchine andrà fatta utilizzando prese distinte e percorsi fisici distinti per gli alimentatori distinti della stessa macchina.
SF9 – Controllo di temperatura ed umidità delle sale macchine	La temperatura ed umidità delle sale macchine devono essere controllate in automatico e programmate in modo che le macchine possano lavorare in un ambiente idoneo. I condizionatori saranno soggetti a manutenzione programmata.
	Per ogni banca dati contenente dati personali o sensibili vanno predisposte opportune procedure di salvataggio periodico che

SF10 – Esecuzione backup	prevedano la frequenza con cui effettuare i backup, la designazione di chi deve eseguire o controllare tali salvataggi, i luoghi ed i criteri di conservazione dei supporti ausiliari di memorizzazione utilizzati per queste attività.
SF11 – Attivazione Procedure di Disaster Recovery	Va predisposta una procedura di Disaster Recovery per i server principali che preveda: il ripristino della banca dati e l'attivazione di server sostitutivi.
SF12 – Armadi ignifughi	I supporti ausiliari di memorizzazione contenenti backup o copie che consentono il restore delle macchine o di database devono essere conservati in armadi ignifughi o casseforti ignifughe oppure in stanze chiuse a chiave.
SF13 – Ridondanza dei sistemi (server)	I server sanitari ed amministrativi che supportano le procedure strategiche per l'Azienda devono prevedere configurazioni ridondanti per quanto riguarda le macchine (cluster), i dischi (RAID), i controller dei dischi nel caso di utilizzo di rack esterni, e possibilmente anche i bus di comunicazione interni, gli alimentatori, le interfacce di rete.
SF14 – Ridondanza delle apparecchiature di rete	Le apparecchiature di rete dei nodi fondamentali preferibilmente prevedranno delle configurazioni in cluster.
SF15 – Ridondanza delle reti WAN	Le linee Wan che collegano tra di loro sedi che prevedono una comunicazione di tipo strategico, vanno ridondate in modo da consentire una via alternativa di comunicazione, sia pure con prestazioni minori; per le altre linee va previsto un contratto di assistenza che assicuri il ripristino entro la giornata lavorativa.
SF16 – Assistenza tecnica	Per i server principali e le apparecchiature di rete LAN va previsto un contratto di assistenza che garantisca un intervento, in caso di guasto, in 4 ore lavorative.

10.3. Misure di sicurezza di tipo logico di mantenimento

DESCRIZIONE MISURA	NOTE ED INDICAZIONI PER LA CORRETTA APPLICAZIONE
SL1 – Codici identificativi personali	I codici identificativi personali vanno distribuiti agli incaricati, conformemente alla attuale normativa. Vanno catalogate le distinte basi di dati (database) in cui tali codici identificativi sono registrati, in modo da identificare la banca dati delle login / password.
SL2 – Predisposizione ed aggiornamento antivirus	Predisporre un sistema antivirus il quale permetta di ottenere la copertura antivirus maggiore possibile, curando in particolare: il controllo di tutte le possibili vie di accesso dei virus al sistema informatico aziendale (varie porte o servizi della rete e dei server, con particolare attenzione alla posta elettronica ed alla navigazione web), nonché l'aggiornamento continuo delle marcature antivirali, con distribuzione automatica a tutti i client mediante agenti automatici sui singoli client e schedulazioni sui server antivirus.
SL3 – Realizzazione di sistemi antintrusione sulle linee di comunicazione verso internet	Le linee di comunicazione verso Internet vanno protette mediante uno o più livelli di firewall, utilizzando le seguenti politiche di sicurezza: • è negato tutto ciò che non è esplicitamente ammesso; • in caso di caduta o guasto del firewall, tutte le • comunicazioni sono bloccate; • tutte le comunicazioni sono attivate solo se partono da una richiesta interna; • sono attivate solo le porte rigorosamente

	necessarie per i servizi essenziali; • sono bloccate le porte utilizzabili per lo scarico o la trasmissione o la condivisione di files peer to peer; • nel caso di utilizzo di comunicazioni attraverso Internet, si utilizzeranno dispositivi capaci di generare collegamenti VPN, attivati solo tramite richiesta formale.
SL4 – Monitoraggio delle intrusioni e dei comportamenti anomali in rete	Il sistema Firewall Aziendale avrà le specifiche tecniche e le funzionalità predisposte per il monitoraggio dei tentativi di intrusione. Sarà inoltre disponibile ed attivabile un sistema IDS Snort. Mediante tali sistemi si intendono individuare tipologie di connessione che possono causare problemi alla rete, sia connessioni non autorizzate a computer o server, sia attività virale o di back-door sfuggita al controllo antivirus, sia la presenza di programmi non autorizzati che vengano attivati sulla rete aziendale.
SL5 – Personal Computer con Sistemi operativi obsoleti	Poiché i sistemi operativi Windows95 e Windows98 permettono un livello di sicurezza sensibilmente minore rispetto a Windows 2000, Xp e 2003, mentre si procede alla loro graduale sostituzione, se ne consente l'utilizzo solo come semplice "terminale" per collegarsi ai server centrali, con le modalità emulazione di terminale (es. VT100) o utilizzando Client di tipo Citrix Metaframe; si fa divieto di depositare files o archivi locali entro tali computer.
SL6 – Aggiornamento (patch) dei software di sistema, di database, applicativi e di rete	Si provvederà all'aggiornamento dei sistemi operativi, del software di database e del software applicativo, compatibilmente con la verifica e la certezza che il nuovo software appena rilasciato non crei nuovi problemi o blocchi al sistema informatico attuale, del quale va garantito il funzionamento (disponibilità).

	Tale fase è particolarmente critica in quanto sperimentalmente non vi è la garanzia che la mera applicazione di una "patch" di aggiornamento non possa bloccare servizi fortemente interconnessi ed interdipendenti.
SL7 – Manutenzione dei database	Si procede alla manutenzione preventiva delle basi di dati; tale manutenzione consiste nella verifica almeno settimanale dello stato del database mediante le console di monitoraggio e management allo scopo attivate, nonché alla periodica ricostruzione di tabelle ed indici che presentino problemi o frammentazioni eccessive. Si prevede di ricorrere anche a strumenti che verifichino la modalità con cui gli applicativi utilizzino il database, e periodicamente anche a consulenze specialistiche di tuning.
SL8 – Manutenzione dei sistemi operativi	Si procede alla manutenzione dei sistemi operativi, monitorandone il funzionamento mediante gli opportuni strumenti di console, verificando i log, configurando i parametri e sorvegliando i processi attivi. Le patches andranno installate solo dopo test che assicurino la continuità del servizio.
SL9 – Individuazione dei criteri di cifratura	I criteri di cifratura o altre misure atte a rendere temporaneamente non intelligibili i dati sensibili o giudiziari
SL10 – Test degli applicativi	Si effettuerà il Test degli applicativi, in ambiente di prova, prima della messa in produzione degli stessi.
SL11 – Test delle modifiche	Si effettuerà il Test delle modifiche dei software, in ambiente di prova, prima della messa in produzione degli stessi. Verifica della permanenza delle modifiche precedentemente introdotte e volute, e delle funzionalità correlate.
	Ove possibile si guiderà l'incaricato del trattamento all'utilizzo di una procedura

SL12 – Controlli di validità	informatica, mediante menù ed opzioni di scelta per l'introduzione dei dati, in modo da garantirne la correttezza e coerenza, per quanto possibile. Si utilizzeranno il più possibile tabelle di codifica, con controlli di coerenza dei dati.
SL13 – Protezione dei computer con i programmi informatici attivi	L'incaricato del trattamento avrà cura di non lasciare incustodito il computer avente programmi attivi e connessi ai server centrali; nel caso si allontani dal computer avrà cura di terminare le sessioni aperte, sia per ragioni di sicurezza che di privacy, che per non impegnare inutilmente le risorse dei sistemi. In modo analogo, nel caso di protezione di files mediante sistemi crittografici, l'incaricato avrà cura di non lasciare aperti i files e di pulirele password dalle memorie caches del computer. Una misura complementare potrà essere l'attivazione di una password sullo salvaschermo.
SL14 – Policy Antivirus	Attivazione di tutte le policy necessarie, rese disponibili dal sistema in rete, calibrate in modo che non vengano bloccate le attività utili, ed in particolare con: 1) una funzionalità di firewall locale sulle porte normalmente utilizzate dai motori virali per aprire backdoor o per attivare collegamenti; 2) controllo o blocco della possibilità del lancio di applicativi o files dalle cartelle temporenee o dal download da parte di applicativi quali Explorer, Outlook Express, MSN, Packager, 3) WinZip, WinRar; 4) Blocca l'accesso a oggetti di startup sospetti (*.exe, *.scr, *.hta, *.com, *.pif); 5) controllo o blocco del tftp.exe, usato da alcuni worm; 6) controllo o blocco della possibilità di

	modificare files da remoto (*.exe, *.dll, *.scr, *.ocx, *.pif); 7) controllo o blocco della possibilità di creazione/modifica/cancellazione di nuovi files nelle cartelle Windows e system root; 8) Blocca la creazione di files *.exe ed *.dll nelle cartelle Windows e System32; 9) Attivare la protezione buffer overflow in locale; 10) Attivare la protezione da: Spyware, Adware, Remote Administration Tool, Dialers, Password Crackers, Jokes. Saranno comunque verificate ed eventualmente adottate le configurazioni di controllo consigliate dai produttori di Antivirus, poiché le minacce sono variabili nel tempo, sia per tipologia che per tecnologia.

10.5. Misure di sicurezza di tipo organizzativo di mantenimento

DESCRIZIONE MISURA	NOTE ED INDICAZIONI PER LA CORRETTA APPLICAZIONE
SO1 – Direzione Aziendale	La direzione aziendale sosterrà e renderà nota la politica sulla sicurezza informatica.
SO2 – Nomina dei Responsabili del Trattamento	Sono nominati responsabili del trattamento, ai fini del D.Lgs. 30 giugno 2003, n.196, i responsabili dei centri di responsabilità dell'Azienda. Tale nomina va comunicata per iscritto.
SO3 – Documento Programmatico sulla Sicurezza e Regolamento per l'accesso al	A cura del Titolare del Trattamento e da predisporre entro il mese di Marzo di ogni anno.

sistema e politiche informatiche aziendali	
SO4 - Sorveglianza	I locali delle sedi aziendali vanno controllati periodicamente da un servizio di "security" durante gli orari non lavorativi.
SO5 – Custodia degli archivi cartacei	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 o documenti sono custoditi dagli incaricati in modo che ad essi non accedano persone prive di autorizzazione. L'accesso agli archivi contenenti dati sensibili o giudiziari va controllato; le persone che vi accedono sono preventivamente autorizzate.
SO6 – Custodia di documenti/dati memorizzati su supporti informatici di vario tipo	I supporti ausiliari di memorizzazione vanno conservati in cassaforte o armadio chiuso a chiave o in locale chiuso a chiave. Quelli non utilizzati vanno distrutti. Le chiavi vanno opportunamente gestite in modo che vengano in possesso solo delle persone autorizzate e che non vi siano blocchi dei servizi erogati.
SO7 – Procedure di accesso ad archivi fisici contenenti dati conservati su supporto cartaceo e/o informatico	Vanno verificate le procedure di accesso agli archivi fisici ed informatici in modo da individuare eventuali punti di debolezza da rinforzare.
SO8 – Piano di verifica delle misure adottate	La bontà delle misure adottate va verificata in modo periodico attraverso Verifiche Ispettive da parte di tecnici opportunamente designati. Va predisposta una apposita ckeck-list, che si ispirerà alla best practice in materia di sicurezza informatica e di privacy, ed alla normativa vigente. Durante queste operazioni di verifica sarà data particolare importanza a: - verificare la bontà delle misure antintrusione adottate - aggiornamento dei dispositivi antivirus - verifica della gestione dei login e

	password - integrità dei dati e delle loro copie di back-up e verifica dell'effettuazione delle stesse - bontà della conservazione dei documenti cartacei - accertamento della distruzione dei supporti magnetici – o comunque dei supporti ausiliari di memorizzazione – che non possono più essere utilizzati.
SO9 – Piano di recupero (dopo un incidente)	Va predisposto un piano il quale indichi, per i server principali dell'Azienda (sanitari relativi ai dati dei ricoveri, cup, anagrafe ed amministrativi relativi ai dati di contabilità, bilancio, gestione del personale, controllo di gestione), come comportarsi per un corretto ripristino in caso di problemi o incidenti che coinvolgano il sistema informatico. Periodicamente va effettuato un test di ripristino dei dati memorizzati nei supporti di backup.
SO10 – Formazione per gli utenti dei sistema informatico aziendale	Si provvederà, conformemente a quanto indicato dal testo unico D.Leg. 30 giugno 2003 n.196, a fornire interventi formativi a più livelli: - dando a tutti gli incaricati precise istruzioni circa l'adozione delle necessarie cautele per la custodia delle chiavi e dei dispositivi; - dando una informazione di base sulla sicurezza informatica agli incaricati individuati; - comunicando e spiegando ai responsabili dei centri di responsabilità nozioni base sulla sicurezza ed il Piano sulla sicurezza informatica dell'Azienda; - provvedendo a dare indicazioni operative adeguate all'assunzione o al cambio di mansioni di un incaricato.

SO11 – Assistenza per gli utenti del sistema informatico aziendale	Il Servizio per l'Informatica, per quanto di sua competenza, attiva dei numeri telefonici per fornire assistenza telefonica competente ed in tempo reale agli utenti del sistema informatico aziendale, in modo anche da garantire il corretto uso degli applicativi. I Numeri telefonici sono pubblicati negli elenchi telefonici dei servizi ed uffici, distribuiti ad ogni reparto, ufficio e servizio.
SO12 – Criteri di protezione nel caso di trattamenti affidati all'esterno	Nel caso di trattamenti di dati affidati all'esterno, si richiederà la certificazione dell'applicazione di tutto quanto previsto dal DL 30 giugno 2003, n.196, in particolare per quel che riguarda la protezione dei dati personali, ed il principio di necessità del trattamento, secondo il quale il trattamento dei dati personali va effettuato utilizzando i dati minimi necessari per raggiungere lo scopo.
SO13 – Disponibilità dei numeri di chiamata per i contratti di assistenza	Presso le sale macchine delle sedi principali saranno disponibili tutti i riferimenti per attivare le chiamate di assistenza (in particolare numeri di contratto di assistenza, macchine interessate, numeri di serie delle macchine e numero telefonico della chiamata, nonché orari del servizio di assistenza e modalità di intervento).
SO14 – Controllo delle nuove installazioni	Tutte le nuove installazioni sono autorizzate o controllate per le specifiche tecniche da un servizio interno, in particolare dal Servizio per l'Informatica.

10.6. Misure di sicurezza di tipo organizzativo di aggiuntive

DESCRIZIONE MISURA	NOTE ED INDICAZIONI PER LA CORRETTA APPLICAZIONE

SO15 – Nomina amministratori di sistema	**Da effettuare con nomina formale**

SEZIONE 11. VERIFICHE E CONTROLLI

L' Azienda provvede alla pianificazione e all'esecuzione di verifiche volte ad accertare la corretta applicazione delle misure minime di sicurezza adottate.

Almeno una volta all'anno, i Responsabili del trattamento provvedono a verificare l'aderenza dello stato di sicurezza del trattamento dei dati col presente documento. La gestione delle attività di verifica avviene in base a quanto riportato nel Regolamento della Policy Aziendale per l'utilizzo degli strumenti elettronici.

Oggetto delle verifiche è:

- **la documentazione,**
- **aggiornamento dell'elenco dei trattamenti,**
- **verifica presenza e adeguatezza delle misure da adottare,**
- **grado di formazione informazione degli incaricati del trattamento,**
- **lo stato di identificazione di documenti e dati,**
- **le attività di conservazione ed archiviazione dei dati e dei documenti,**
- **la conduzione della esecuzione delle attività lavorative, tenendo conto della conformità ai requisiti imposti dal "Codice in materia di protezione dei dati personali".**

Per ogni caratteristica per la quale si riscontra una insufficiente applicazione (giudizio negativo), il Titolare del trattamento deve necessariamente definire un piano e le tempistiche di risoluzione per un rapido rientro della deviazione. Situazioni di non

aderenza per periodi superiori ai sei mesi possono essere accettate solo con autorizzazione scritta da parte del Garante.

È compito dei Responsabili del trattamento, invece, stabilire ed effettuare controlli periodici nell' Azienda e presso gli outsourcer esterni che trattano dati personali, al fine di stabilire lo stato di sicurezza. Almeno semestralmente dovranno presentare al Titolare del trattamento un rapporto sullo stato di sicurezza rilevato.

Nel caso in cui siano rilevati scostamenti rispetto al DPS, i Responsabili del trattamento o l'Amministratore di sistema potranno stabilire adeguati piani correttivi, notificando al Titolare del trattamento la situazione e tenendolo aggiornato sull'applicazione del piano stesso.