Documento Programmatico sulla Sicurezza dei dati personali e sensibili

DPS 2011

Redatto in base alla disposizione di cui al punto 19 del

DISCIPLINARE TECNICO IN MATERIA di MISURE MINIME di SICUREZZA

del

CODICE IN MATERIA di PROTEZIONE DEI DATI PERSONALI (D,lgs. n. 196 del 30 giugno 2003)

in collaborazione con la Società Systema Consulting di Roma

INDICE DELLE REVISIONI

DPS
Documento programmatico sulla sicurezza

31/03/2011	7	Aggiornamento Allegati e DPS	Approvato Delib N.
Data rev.	rev.	Descrizione della Revisione	Rif. delibera del Titolare del Trattamento

LISTA DI DISTRIBUZIONE DEL DPS			
RSDP	**RSPT**	**GLP**	

ALLEGATI
Vedi elenco degli allegati a pag. 2

ELENCO DEGLI ALLEGATI

	Codice Documento	ALLEGATI AL DPS
☒	ALL_A1	Elenco dei trattamenti gestiti senza l'ausilio di strumenti elettronici
☒	ALL_A2	Elenco dei trattamenti gestiti con l'ausilio di strumenti elettronici
☒	ALL_A3	Elenco dei trattamenti raggruppati per ufficio / reparto di trattamento
☒	ALL_B	Elenco delle sedi e degli uffici/reparti in cui vengono trattati i dati
☒	ALL_D	Elenco dei sistemi di elaborazione per il trattamento dei dati
☒	ALL_E	Elenco Trattamenti in outsourcing
☒	ALL_H	Piano di formazione del personale autorizzato al trattamento dei dati
☒	ALL_ITD1	Elenco degli incaricati del trattamento per Reparto/Ufficio e incarico omogeneo
☒	ALL_O	Opuscolo informativo per il personale
☐	ALL_ISM	Incaricati del servizio di manutenzione degli strumenti elettronici
☒	ALL_ADS	Elenco Amministratori di Sistema
☒	ALL_BKP	Elenco incaricati delle copie di sicurezza delle banche dati
☒	ALL_RSDT	Elenco dei responsabili della sicurezza del trattamento dei dati personali
☒	ALL_RESTD	Elenco dei responsabili esterni del trattamento dei dati personali
☒	ALL_TEC	Relazione annuale sullo stato dei rischi ed eventuali contromisure da adottare
☒	Regolamento	Regolamento ai sensi dell'art. 20 comma 2 del D.Lgs. 196/2003
☒	ALL_LXA	Testo del DLgs. n. 196 del 30 giugno 2003
☒	ALL_LXB	Allegato B al DLgs n. 196 del 30 giugno 2003
☒	ALL_LXC	Amministratori di Sistema
☒	ALL_PO01	Linea Guida per i trattamenti dei dati personali con strumenti elettronici
☒	ALL_PO02	Linea Guida per le Verifiche Ispettive Interne per i Trattamenti di Dati Personali
☒	ALL_PO03	Regolamento per l'utilizzo degli impianti di videosorveglianza

Tabella Allegati al DPS (solo i documenti spuntati sono compilati)

Codice Documento	MODULI PER LA RACCOLTA DEI DATI
TTR1	Fac-Simile del Modulo di segnalazione cessazione o avvio di un trattamento
AIT01	Fac-Simile del modulo per la comunicazione delle autorizzazioni al trattamento
CIT01	Fac-Simile del modulo per la comunicazione della per perdita della qualità di incaricati
CM070	Fac-Simile Piano verifiche ispettive
CM071	Fac-Simile Rapporto di verifica ispettiva
CM072	Fac-Simile Segnalazione di non conformità
CM073	Fac-simile Comunicazione Banche dati e nominativi Incaricati del Trattamento

Tabella dei moduli per la registrazione o comunicazione dei dati

INDICE DEI CAPITOLI

1 Introduzione e riferimenti

1.1 Scopo

Il presente Documento Programmatico Sulla Sicurezza è redatto per soddisfare tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)**.
Inoltre costituisce un valido strumento per la adozione delle misure previste **dall'Art. 31, dall'Art. 34 e dall'Art. 35** dello stesso **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)**.
Scopo del presente Documento programmatico sulla sicurezza è quello di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

1.2 Campo di applicazione

Il Documento Programmatico Sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il Documento programmatico sulla sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.3 Riferimenti Normativi

Il presente documento è stato redatto in conformità al D.Lgs. n. 196 del 30 giugno 2003 e del disciplinare tecnico in materia di misure minime di sicurezza (allegato B al DLgs. n. 196 del 30 giugno 2003).

1.4 Termini e Definizioni

In questo paragrafo sono descritti alcuni dei termini e definizioni utilizzati nel documento.

1.4.1 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.

1.4.2 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.

1.4.3 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.

1.4.4 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.

1.4.5 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.

1.4.6 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.

1.4.7 Incaricati

Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

1.4.8 Interessato

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

1.4.9 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.

1.4.10 Diffusione

Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.4.11 Dato anonimo

Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.4.12 Blocco

La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

1.4.13 Banca dati

Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

1.4.14 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.

1.4.15 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.

1.4.16 Strumenti elettronici

Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

1.4.17 Autenticazione informatica

L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

1.4.18 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.

1.4.19 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.

1.4.20 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.

1.4.21 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.

1.5 Regole per il trattamento per i soggetti pubblici

1.5.1 Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici

Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

La comunicazione e la diffusione sono vietate

E' fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

1.5.2 Principi applicabili al trattamento di dati diversi da quelli sensibili

La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2 del DLgs. 196/03, e non è stata adottata la diversa determinazione ivi indicata.

La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

1.5.3 Principi applicabili al trattamento di dati sensibili

1) Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2) Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), del DLgs 196/03 anche su schemi tipo.

3) Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2 del DLgs 196/03, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma al precedente punto precedente.

1.5.4 Principi applicabili al trattamento di dati giudiziari

Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

1.6 Acronimi e abbreviazioni

I sottoelencati termini potranno essere utilizzati, nei richiami successivi, indipendentemente nella forma estesa od in quella abbreviata.

1.6.1 Funzioni aziendali ai fini della sicurezza dei dati personali

TTRA	**T**itolare del **TRA**ttamento
GLP	**G**ruppo di **L**avoro **P**rivacy
RSTD	**R**esponsabile della **S**icurezza **T**rattamento **D**ati personali
RESTD	**R**esponsabile **E**sterno **S**icurezza **T**rattamento **D**ati personali
RSPT	**R**esponsabile di **SP**ecifico **T**rattamento di dati personali
ISM	**I**ncaricati del **S**ervizio di **M**anutenzione degli strumenti elettronici
ADS	**A**mministratore di **S**istema
ICCC	**I**ncaricato della **C**ustodia delle **C**opie delle **C**redenziali
ICSD	**I**ncaricato **C**opie di **S**icurezza delle banche **D**ati
RTDO	**R**esponsabile del **T**rattamento **D**ati in **O**ut-sourcing
TAUT	**T**itolare **AUT**onomo
ITDP	**I**ncaricato **T**rattamento dei **D**ati **P**ersonali
UFAP	Responsabile **U**fficio **F**ormazione **A**ggiornamento **P**rofessionale

1.6.2 Abbreviazioni e acronimi

ALL Allegati al DPS

DPS **D**ocumento **P**rogrammatico sulla **S**icurezza

1.7 Organizzazione, ruoli e compiti delle figure aziendali per la sicurezza dei dati personali

I contenuti delle posizioni organizzative sono descritti al cap. 5 del **DPS** nella sezione dedicata all' Organizzazione ; conformemente al punto 19.2 del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003).** l'attribuzione di compiti e delle responsabilità per l'esecuzione delle attività e le attività stesse sono inoltre richiamate nei singoli capitoli del **DPS**.

2 Organizzazione e modalità di gestione del documento

In questo capitolo è spiegata l'organizzazione strutturale del documento e le modalità con cui viene gestito.

2.1 Organizzazione del documento

Il presente documento è strutturato su 4 livelli così denominati:

- capitoli
- sezioni
- paragrafi
- sottoparagrafi

2.2 Emissione del DPS

Il **DPS** è emesso dal **TTRA** in collaborazione con il **GLP**.

2.3 Compilazione degli allegati al DPS

Quando ne sussistono le condizioni , o quando ritenuto necessario e comunque almeno 1 volta all'anno il **GLP** aggiorna tutti gli **ALL**.

2.4 Gestione delle revisioni

Il documento viene revisionato con periodicità indicata nel *punto 2.9 del presente capitolo e quando il titolare del trattamento lo ritiene necessario al fine di migliorare l'efficienza del sistema di protezione dei dati personali*. Il Titolare del Trattamento provvederà a revisionare il **DPS** con formale atto deliberativo i cui estremi sono riportati nel frontespizio del DPS. Al momento della revisione vengono aggiornati anche il numero e la data di revisione indicando una breve descrizione delle modifiche intervenute sul documento.
Ogni anno, almeno 30 giorni prima del 31 marzo, i **RSTD** trasmettono i dati aggiornati al **GLP** per permettere l'aggiornamento del **DPS**.

2.5 Gestione delle distribuzioni

Il DPS viene distribuito a tutti i membri indicati nel frontespizio del **DPS** stesso ogni volta che questo viene revisionato. La distribuzione del **DPS** è gestita da **GLP.**

2.6 Archiviazione e Conservazione

GLP - è responsabile dell'archiviazione e conservazione del **DPS**, e degli **ALL**

2.7 Responsabilità

Responsabile dell'emissione e aggiornamento del **DPS** è il **TTRA** in collaborazione con il **GLP**
Responsabile dell'archiviazione e della distribuzione del **DPS** è il **GLP**
Responsabile dell'approvazione del **DPS** è il **TTRA**
Responsabile dell'archiviazione delle copie delle lettere d'incarico è il **GLP**

2.8 Periodicità di revisione del DPS

Entro il 31 marzo di ogni anno, il **Titolare del trattamento** di dati sensibili o di dati giudiziari deve verificare ed aggiornare il **Documento programmatico sulla sicurezza.**

2.8.1 Relazione del bilancio d'esercizio

Con riferimento al **punto 26 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003),** nel caso in cui è previsto che debba essere redatta la **Relazione accompagnatoria al Bilancio d'esercizio** il **Titolare del trattamento** deve riferire della avvenuta redazione o dell'avvento aggiornamento del Documento programmatico sulla sicurezza nei termini previsti e ne attesti la conformità a quanto stabilito dal **Codice in materia di protezione dei dati personali.**

3 Trattamenti con l'ausilio di strumenti elettronici

3.1 Sistema di autenticazione informatica

In conformità a quanto disposto dal **punto 1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, il **RSTD** deve assicurarsi che il trattamento sia consentito solamente agli **Incaricati del trattamento dei dati personali** 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.

3.2 Identificazione dell'incaricato

In conformità a quanto disposto dal **punto 2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** il **RSTD** avvalendosi della collaborazione dell'**Incaricato della custodia delle copie delle credenziali** e dell'**ADS** deve assicurare che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli **Incaricati del trattamento** dotati di una o più **Credenziali di autenticazione** tra le seguenti:

- Un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo
- Un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave
- Una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

In conformità a quanto disposto dal **punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** ad ogni **Incaricato del trattamento** possono essere assegnate o associate individualmente una o più **Credenziali per l'autenticazione**.

3.2.1 Criteri di assegnazione delle password di accesso agli strumenti elettronici

Su ogni strumento vengono creati gli utenti senza diritti amministrativi ognuno con una password personale che viene consegnata la prima volta in busta chiusa. L'utente alla prima connessione ha l'obbligo di cambiarla in quanto il sistema stesso lo obbliga a farlo. L'impostazione delle policy di sicurezza del sistema prevede che la password sia lunga almeno 8 caratteri alfanumerici. Lo strumento è impostato in modo da fare scadere la password dopo 90 gg. e costringere l'operatore a sostituirla.

Tutti i PC sono impostati con lo screen saver che rimanda alla Login non oltre i 5 minuti di inattività.

La procedura per l'assegnazione delle credenziali di autenticazione sono anche indicate nelle Linee Guida per i trattamenti di dati personali con strumenti elettronici (**PO01**) allegate al presente **DPS**

3.2.2 Criteri di assegnazione delle password di accesso ai software sanitari

Le password di accesso ai software viene rilasciata dal personale che gestisce il software o dalla ditta appaltatrice della manutenzione del software. E' previsto il cambio della password

ogni 90 giorni. Gli amministratori di sistema (**ADS**) sono in grado di sostituire la password scelta dall'utente dopo che questi l'ha cambiata ma non di recuperarla.

3.3 Cautele per assicurare la segretezza della componente riservata della credenziale

In conformità a quanto disposto dal **punto 4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** gli incaricati debbono adottare le necessarie cautele per assicurare la segretezza della **parola chiave** e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..).
Inoltre ogni **Incaricato del trattamento** è informato e reso edotto che le **Credenziali di autenticazione**:

- Sono personali
- Devono essere memorizzate
- Non devono essere comunicate a nessuno
- Non devono essere trascritte

3.4 Caratteristiche della parola chiave

In conformità a quanto disposto dal **punto 5 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** la **Componente riservata delle credenziali di autenticazione** (parola chiave o password) deve rispettare i seguenti criteri:

- Non deve contenere nomi comuni
- Non deve contenere nomi di persona
- Deve contenere sia lettere che numeri
- Deve essere diversa dallo User-Id (nome utente)
- Deve essere lunga 8 caratteri o massimo consentito dal sistema di autenticazione
- Non deve essere riconducibile all'incaricato

3.5 Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico

In conformità a quanto disposto dal **punto 9 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** gli **Incaricati del trattamento** hanno l'obbligo di:

- Non lasciare incustodito il proprio posto di lavoro.
- Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.
- Di adottare tutte le cautele necessarie atte ad evitare accessi ai dati non consentiti

3.6 Accesso straordinario

In conformità a quanto disposto dal **punto 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** gli **Incaricati della custodia delle copie delle credenziali (ICCC)**, hanno il compito di assicurare la disponibilità dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
La custodia delle copie delle **Credenziali di autorizzazione** è organizzata garantendo la relativa segretezza.

Gli **Incaricati della custodia delle copie delle credenziali** devono informare tempestivamente l'**Incaricato del trattamento** ogni qualvolta sia stato effettuato intervento straordinario in sua assenza.
In conformità a quanto disposto dal **punto 11 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** 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.

3.6.1 Modalità di accesso straordinario in caso di inderogabili necessità e indisponibilità dell'incaricato

Nella quasi totalità dei casi la figura dell'**ICCC** è sostituita da **ADS** il quale in dipendenza del tipo di accesso da garantire dispone specifiche procedure. Fatta eccezione per i software che non prevedono un accesso amministrativo per impostare le credenziali di accesso, l'accesso straordinario è garantito con una semplice procedura che prevede la sostituzione della password dell'utente incaricato assente con una password amministrativa temporanea. Tale procedura prevede che l'amministratore di sistema (**ADS**) al termine delle operazioni ritenutesi urgenti durante l'assenza dell'incaricato informi quest'ultimo dell'avvenuto accesso straordinario e della necessità quindi di sostituire la componente riservata delle credenziali con una segreta di esclusiva conoscenza dell'incaricato
I software che non prevedono un accesso amministrativo verranno gestiti con il sistema delle buste chiuse in custodia ad **ICCC** o **ADS**

3.6.2 Modalità di accesso straordinario al sistema per operazioni di manutenzione

ADS in collaborazione con **ISM** ha creato su ogni PC un utente administrator con una password convenuta dai responsabili ad uso esclusivo di operazioni di gestione amministrativa o tecnica dello strumento. Tale password viene utilizzata esclusivamente per operazioni di carattere tecnico quali l'installazione di nuove applicazioni, aggiornamenti hardware e altre operazioni di manutenzione.

3.6.3 Modalità di accesso straordinario ai software sanitari

Il personale tecnico che gestisce e mantiene il software ha la possibilità di avere accesso alle informazioni. Tali accessi devono avvenire solo su richiesta ed in presenza del **RSTD** o dell'**incaricato al trattamento** e solo in caso sia impossibile avere accesso in altro modo per assenza dell'incaricato o guasto del sistema.

3.7 Sistema di Autorizzazione

Il **RSTD** ha il compito di individuare gli **Incaricati del trattamento** per ogni tipologia di banca di dati personali trattata.
In conformità a quanto disposto dal **punto 12** e dal **punto 13 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** il tipo di trattamento effettuato da ogni singolo **Incaricato del trattamento** può essere differenziato.
In particolare il **RSTD** può decidere quali operazioni di trattamento siano consentite ad ogni **Incaricato del trattamento** tra le seguenti:

- Consultare le informazioni nella banca di dati personali
- Inserire nuove informazioni nella banca di dati personali
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella banca di dati personali
- Cancellare le informazioni esistenti nella banca di dati personali

In conformità a quanto disposto dal **punto 15 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** almeno una volta l'anno e comunque **entro il 31 marzo**, ogni **RSTD** deve aggiornare l' **ELENCO INCARICATI AL TRATTAMENTO DEI DATI PERSONALI NELL'UFFICIO/REPARTO E I PERMESSI DI ACCESSO ALLE BANCHE DATI** che sono stati assegnati agli **Incaricati del trattamento** per ogni tipologia di banca di dati. La comunicazione di variazioni deve essere data tempestivamente a **ADS** o **ISM** che provvederà a modificare il sistema di autorizzazione.
In conformità a quanto disposto dal **punto 19.2 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003), l'allegato **ALL_IDT** contenente l'elenco degli incaricati al trattamento e l'allegato **ALL_ITD1** contenente l'elenco degli incaricati del trattamento dei dati personali per ufficio/reparto deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.7.1 Modalità di gestione delle autorizzazioni

L'elenco degli incaricati del trattamento viene redatto per classi omogenee di incarico come previsto al **punto 15 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003).** In funzione di ciò il sistema di autorizzazione viene configurato sugli strumenti per il trattamento e sui server in modo da consentire l'accesso ai dati agli incaricati del trattamento per reparto/ufficio di competenza. **RSTD** trasmette a **ADS** le modifiche da effettuare al sistema di autorizzazione con i nominativi degli incaricati. La frequenza della comunicazione è annuale o tempestiva nel caso un incaricato perda le qualità che permettono a quest'ultimo l'accesso ad uno o più trattamenti.
La comunicazione avviene attraverso il modulo **AIT01** il cui fac-simile è allegato al presente **DPS**.
ADS potrà sviluppare sistemi informatici on line in modo da acquisire i dati del modello **AIT01** attraverso la intranet aziendale e quindi rendere tempestiva la comunicazione.

3.8 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

3.8.1 Riferimenti normativi

La Sezione è redatta in conformità al **punto 14 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)**

3.8.2 Modalità operative

RSTD in collaborazione con i **ADS** ha il compito di verificare ogni anno, **entro il 31 marzo**, le **Credenziali di autenticazione**.

3.8.2.1 Modalità di Assegnazione delle credenziali di autenticazione

I criteri e le periodicità con cui vengono assegnate e aggiornate le credenziali di autenticazione per l'accesso ai dati sono stabiliti nell' **ALL_PO01** allegato al presente documento. Le variazioni al sistema di autorizzazione vengono riportati all'**ALL_IDT** e **ALL_IDT1** in quanto contenenti rispettivamente la lista aggiornata degli incaricati e degli incaricati per ufficio/reparto con l'indicazione delle banche dati. Le modalità per le segnalazioni di variazione sono indicate al precedente punto 3.7.1.

3.9 Elenco delle sedi e degli uffici in cui vengono trattati i dati

3.9.1 Riferimenti normativi

La Sezione è redatta in conformità al **punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)**

3.9.2 Modalità operative

Ad ogni **RSTD** è affidato il compito di comunicare al **GLP** ogni variazione riguardo l'elenco delle sedi e degli uffici/reparti di competenza in cui viene effettuato il trattamento dei dati. La sede di competenza è indicata nella lettera d'incarico che segue la delibera di nomina a Responsabile della sicurezza dei dati personali.
L'elenco delle Sedi e degli uffici in cui sono trattati dati è riportato nell'allegato **ALL_B** compilato da **GLP** e che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

GLP aggiorna nell' **ALL_B** l'elenco delle strutture in cui avviene il trattamento dei dati ed ha assegnato ad ogni struttura un codice univoco da utilizzare come riferimento e/o prefisso per la compilazione di altri allegati.

3.10 Elenco dei trattamenti e degli archivi dei dati oggetto del trattamento

3.10.1 Riferimenti normativi

La Sezione è redatta in conformità al **punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)**

3.10.2 Elenco dei Trattamenti

In questa sezione sono individuate le modalità per il censimento dei trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna od esterna operativamente preposta, nonché degli strumenti elettronici impiegati.

3.10.2.1 Censimento dei trattamenti

L'Azienda realizza il censimento dei dati personali e/o sensibili (anagrafe).
Il censimento contiene la rilevazione dei trattamenti dei dati suddivisi per categorie e per strutture organizzative.

3.10.2.2 Modalità Operative

Ad ogni **RSTD** è affidato il compito di comunicare al **GLP** ogni variazione dei trattamenti effettuati all'interno della struttura di competenza utilizzando il modulo **TTR1**

Il modulo **TTR1** perviene al **GLP** che provvederà a riesaminare e verificare i dati in modo da inserirlo nell'elenco dei trattamenti. Per ogni trattamento occorre indicare:

- Codice identificativo del trattamento o della banca dati
- La descrizione abbreviata del trattamento o della banca dati
- Tipo di dati trattati : comuni, sensibili o giudiziari
- Il tipo di banca dati (scelto da un elenco predefinito)
- Le finalità del trattamento (scelte da un elenco predefinito)

- Le strutture che sono coinvolte nel trattamento (luoghi di trattamento: reparti, uffici)
- Le categorie di interessati (scelte da un elenco predefinito)
- Le operazioni di trattamento (scelte da un elenco predefinito)
- La modalità di gestione (con strumenti elettronici, cartacea, entrambe)
- Le modalità di assegnazione delle credenziali e la frequenza di aggiornamento delle stesse (indicare il riferimento all'**ALL_PO01** qualora siano standard)
- L'eventuale server di riferimento (chiedere a **ADS** se non è conosciuto)
- L'elenco dei sistemi con cui vengono trattati i dati (indicare il numero identificativo dello strumento: matricola, numero di inventario o altro identificativo)
- Le modalità di backup della banca dati ed i responsabili del backup
- L'elenco degli incaricati (indicare le categorie di incaricati)
- L'elenco degli incaricati della custodia delle copie delle credenziali (per l'accesso allo strumento e ai dati in caso di assenza prolungata dell'incaricato)

L'elenco di tutti i trattamenti aggiornato annualmente è riportato nell'allegato **ALL_A** compilato a cura di **GLP** e che deve essere allegato al presente **Documento Programmatico sulla Sicurezza**.

3.10.2.3 Altre Misure di Sicurezza

L'elenco dei trattamenti **ALL_A** e degli uffici reparti in cui avviene il trattamento **ALL_A1** includono anche le categorie di incaricati con il rispettivo profilo di autorizzazione per l'accesso ai dati. Questi documenti costituiscono l'individuazione dell'ambito del trattamento consentito per classi omogenee di incarico come stabilito al **punto 15 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)**

3.11 Elenco dei sistemi di elaborazione per il trattamento

3.11.1 Riferimenti normativi

La Sezione è redatta in conformità al **punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)**

3.11.2 Modalità operative

ADS gestisce la LAN aziendale e tiene sotto controllo il parco macchine con cui vengono eseguiti i trattamenti. Egli programma le attività di manutenzione come stabilito nell'**ALL_PO01** dei sistemi e provvede all'aggiornamento dell'elenco dei sistemi di elaborazione con cui avviene il trattamento dei dati personali. Ogni anno entro il 28 febbraio trasmette l'elenco dei sistemi di elaborazione aggiornato al **GLP**. Tale documento costituisce l'allegato **ALL_D** e deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.12 Distribuzione dei compiti e delle responsabilità

3.12.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 19.2 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003).

3.12.2 Modalità operative

L'Organigramma funzionale ai fini della gestione del sistema di protezione dei dati personali**,** sono riportati dal **GLP** nel modulo **ALL_J** che deve essere allegato al presente Documento Programmatico sulla Sicurezza.
CODAP definisce e identifica i ruoli, compiti e responsabilità per le figure in organigramma nel presente **DPS**.

3.12.3 Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali

Le modalità operative per le nomine delle figure previste per la sicurezza dei dati personali e la descrizione delle responsabilità e dei compiti sono dettagliatamente descritti al capitolo 5 del presente documento.

3.13 Analisi dei rischi

3.13.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196/2003).

3.13.2 Analisi dei rischi hardware

ADS deve verificare ogni anno:

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- La sicurezza dei dati trattati
- Il rischio di distruzione o di perdita
- Il rischio di accesso non autorizzato o non consentito.

3.13.3 Analisi dei rischi sui sistemi operativi e sui software installati

A **ADS**, è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei software utilizzati.
- Segnalazioni di Patch, Fix o System/Service-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System/Service-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

3.13.4 Analisi degli altri rischi che incombono sui dati

Al **RSTD** in collaborazione con i **Responsabili degli specifici trattamenti di dati personali**, è affidato il compito di analizzare eventuali altri rischi connessi al trattamento dei dati tenendo conto in particolare di:

- Rischi connessi al comportamento degli operatori
- Rischi connessi al contesto fisico ed ambientale

3.13.5 Modalità operative

Il **Responsabile della sicurezza dei dati personali** con la collaborazione di **ADS** deve aggiornare il **Report annuale di tutti i rischi che incombono sui dati (ALL_T).**
Nel modulo su indicato devono essere riportate le seguenti informazioni:

- Descrizione Rischio valutato
- Gravità della minaccia (forte/debole)
- Descrizione dell'impatto che la minaccia ha sui dati
- Descrizione della contromisura
- Efficacia della contromisura adottata o da adottare
- Valutazione del Rischio (alto/medio/basso)
- Data della valutazione
- Data della prossima valutazione
- Rapporto sulla sicurezza

ADS ed i **Responsabili degli specifici trattamenti di dati personali**, nel caso in cui esistano rischi evidenti, debbono informare tempestivamente il **RSTD** affinché siano presi gli opportuni provvedimenti per assicurare la conformità alle norme in vigore e la sicurezza dei dati personali.

3.14 Elenco delle misure da adottare per garantire l'integrità e la disponibilità dei dati

3.14.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 18**, **punto 19.4 e dal punto 19.5 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003).

3.14.2 Modalità operative

RSTD in collaborazione con gli **ADS**, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.
Le linee guida per tali operazioni sono riportate nell'**ALL_PO01**.
I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata e compatibilmente con quanto previsto al **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
ADS, predispone le istruzioni per la copia (backup), verifica e ripristino dei dati. Tali informazioni dovranno essere inviate al **GLP** entro il 28 febbraio di ogni anno e costituiscono l'**ALL_M** che contiene l'elenco delle misure adottate per garantire l'integrità dei dati e che deve essere tenuto aggiornato e allegato al presente Documento Programmatico sulla Sicurezza.

3.14.3 Formazione degli incaricati del backup

Il responsabile **dell'ufficio formazione e aggiornamento del personale** (**UFAP**), deve redigere ogni anno, **entro il 31 marzo**, il **Piano di Formazione degli incaricati dei Backup**

Il Piano di formazione degli incaricati delle copie di sicurezza deve essere predisposto per:

- Rendere edotti gli incaricati sulle modalità tecniche per l'esecuzione delle copie di sicurezza
- Rendere edotti gli incaricati sulla conservazione dei media e sulla loro sicurezza
- Rendere edotti gli incaricati sulle modalità di accesso ai dati
- Rendere edotti gli incaricati sulle modalità di ripristino dei dati in caso di disaster recovery

3.15 Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

3.15.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003),

3.15.2 Misure generali

In considerazione di quanto disposto dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n. 196 del 30 giugno 2003)**, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal **Responsabile della sicurezza dei dati personali** o dal **Responsabile dello specifico trattamento di dati personali** oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personali** o dal **Responsabile dello specifico trattamento di dati personali**, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personali** o dal **Responsabile dello specifico trattamento di dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

3.15.3 Modalità operative

Al **GLP** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati. Ogni incaricato del trattamento e ogni persona all'interno degli uffici e dei locali in cui sono trattati i dati personali ha il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
Ogni incaricato del trattamento che esce dal locale o dall'ufficio in cui sono trattati dati personali lasciandolo incustodito provvede a chiudere la porta a chiave.
Per l'archiviazione e conservazione di documenti cartacei vengono utilizzati ovunque armadi chiusi a chiave e cassettiere con chiusura.

Tutti i locali in cui sono custoditi dati personali sono protetti con chiavi alle porte e armadi con chiusura. Particolari attenzioni sono riservate ai registri di somministrazione di farmaci classificati come stupefacenti che quando possibile sono custoditi in cassaforte altrimenti in armadi chiusi in zone riservate e non accessibili al pubblico.
Nei distretti sanitari e nei presidi ospedalieri esiste un servizio di sorveglianza che controlla gli accessi dei fabbricati.
Le sale server sono protette con porte blindate e nei locali è presente un impianto di allarme centralizzato che viene attivato nelle ore in cui le stanze non sono presidiate dal personale addetto.

Il **RSTD** deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

3.16 Formazione degli incaricati del trattamento

3.16.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 19.6 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003),

3.16.2 Modalità operative

In conformità a quanto disposto dal **punto 19.6 del Disciplinare tecnico in materia di misure minime di sicurezza (Dlgs. n. 196 del 30 giugno 2003)** il **Responsabile della sicurezza dei dati personali**, valuta, per ogni incaricato a cui è stato affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.
La formazione è programmata già al momento dell'ingresso in servizio di nuovi incaricati del trattamento, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il responsabile **dell'ufficio formazione e aggiornamento del personale** (**UFAP**), in base anche alle indicazioni del **GLP** deve redigere ogni anno, **entro il 31 marzo**, il **Piano di Formazione del personale** specificando le necessità di ulteriore formazione del personale.

Il Piano di formazione del personale deve essere predisposto per:

- Rendere edotti gli incaricati del trattamento sui rischi che incombono sui dati
- Rendere edotti gli incaricati del trattamento sulle misure disponibili per prevenire eventi dannosi
- Rendere edotti gli incaricati del trattamento sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività
- Rendere edotti gli incaricati del trattamento sulle responsabilità che ne derivano
- Rendere edotti gli incaricati del trattamento sulle modalità per aggiornarsi sulle misure minime adottate dal titolare

La pianificazione e la registrazione delle attività di formazione viene riportata annualmente nell' **ALL_H** e allegata al presente **DPS.**
Ad ogni revisione annuale del **DPS** viene proposta la bozza del piano di formazione per l'anno successivo e riportata nell'**ALL_H**.

3.17 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

3.17.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003),

3.17.2 Trattamenti di dati personali affidati all'esterno della struttura del titolare

RSTD, può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

3.17.3 Modalità operative

RSTD, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

- I soggetti interessati
- I luoghi dove fisicamente avviene il trattamento dei dati stessi
- I responsabili del trattamento di dati personali

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, deve essere utilizzato il modulo **ALL_E**, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **GLP**, in luogo sicuro.

3.17.4 Criteri per la scelta degli enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare

Il **Responsabile della sicurezza dei dati personali**, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti di esperienza, capacità ed affidabilità individuati all'**art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)**.

3.17.5 Modalità operative

Il Titolare a cui è stato affidato il trattamento dei dati all'esterno deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.

3.17.6 Nomina del responsabile del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, **RSTD** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
La nomina del **Responsabile del trattamento in Out-sourcing** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **RSTD** in luogo sicuro.
RSTD deve informare il **Responsabile del trattamento in Out-sourcing**, dei compiti che gli sono assegnati in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
Il **Responsabile del trattamento in Out-sourcing** deve accettare la nomina.

Al momento dell'affidamento dell'incarico il **Responsabile del trattamento in Out-sourcing**, deve dichiarare per iscritto:

- *Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali*
- *Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali*
- *Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.*
- *Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.*
- *Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.*

3.17.7 Nomina del titolare autonomo del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, **RSTD** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

La nomina del **Titolare autonomo del trattamento in Out-sourcing** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **RSTD** in luogo sicuro.

RSTD deve informare il **Titolare autonomo del trattamento in Out-sourcing**, dei compiti che gli sono assegnati in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.

Al momento dell'affidamento dell'incarico il **Titolare autonomo del trattamento in Out-sourcing**, deve dichiarare per iscritto:

- *Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali*
- *Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali*
- *Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.*

- *Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.*
- *Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.*

3.18 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

3.18.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 16, punto 17, punto 20, punto 21, punto 22, punto 23 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003),

3.18.2 Protezione contro l'accesso abusivo

Al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il **Responsabile della sicurezza dei dati personali**, deve stabilire, con il supporto tecnico degli **ADS**, le misure tecniche da adottare in rapporto ad eventuali rischi.
I criteri debbono essere definiti dal **RSTD** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni Sistema interessato debbono essere definite le seguenti specifiche:

- In conformità a quanto disposto dal **punto 16 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** individuare gli idonei strumenti per la protezione degli strumenti elettronici contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
- In conformità a quanto disposto dal **punto 17 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** stabilire le frequenza con cui aggiornare i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti.
- In conformità a quanto disposto dal **punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** individuare come proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso abusivo da parte di chiunque abusivamente si introduce nel sistema informatico o telematico.

3.18.2.1 Misure da adottare

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 antivirus da aggiornare con cadenza **almeno mensile**.

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati, a cura di **ADS** o da **ISM**, almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è **almeno semestrale**.

Oltre a quanto previsto al punto 3.1 (modalità e criteri di assegnazione delle credenziali di autenticazione) **ADS** o **ISM** provvede ad assicurare la corretta configurazione di ROUTER e

FIREWALL, ovvero di idonei strumenti elettronici allo scopo di garantire un livello di protezione adeguato da eventuali tentativi di accesso abusivo ai sistemi.
Nella relazione annuale sullo stato dei rischi (**ALL_TEC**), **ADS** riporta lo stato del livello di sicurezza dell'infrastruttura informatica riguardo:

- Gestione delle credenziali di autenticazione
- Aggiornamenti del software di base
- Aggiornamenti software applicativo
- Aggiornamenti e disponibilità software antivirus
- Aggiornamenti e monitoraggio dei sistemi antintrusione (firewall)
- Interventi di configurazione effettuati sugli strumenti di sicurezza
- Interventi eseguiti da personale esterno alla struttura
- Adeguatezza dell'hardware
- Adeguatezza dei sistemi utilizzati per le copie di sicurezza
- Adeguatezza infrastrutturale (impianti)
- Report annuale sulla valutazione dei rischi

3.18.2.2 Misure adottate: Antivirus

Ogni strumento in uso è protetto con antivirus con funzione di LIVE UPDATE.

3.18.2.3 Misure adottate: Aggiornamenti del software

L'aggiornamento viene effettuato almeno semestralmente o in modo automatico secondo il sistema in uso. Per i sistemi che non prevedono funzioni di live update tale operazione viene svolta con cadenza quadrimestrale.

Le date stabilite per questa operazione sono:

- dal 1 al 30 gennaio,
- dal 1 al 30 maggio
- dal 1 al 30 settembre

di ogni anno solare o quando l'editore rilascia nuove versioni a correzione delle versioni installate.

L'incaricato della manutenzione delle apparecchiature (**ISM** o **ADS**) in possesso delle password amministrative sarà responsabile dell'effettivo svolgimento dell'operazione di aggiornamento. Ad ogni aggiornamento si tiene traccia dell'operazione svolta su un modulo di registrazione a libero uso di **ISM.**

3.18.2.4 Misure adottate per il rischio esterno: Firewall

Il rischio di intrusione dall'esterno è protetto da firewall sulla dorsale principale. L'azienda ha un accesso unico attraverso una dorsale principale installata presso l'ospedale SAN FRANCESCO. Non sono autorizzati altri accessi al di fuori di questo sistema.
Per gli utenti che non sono connessi alla WAN aziendale il firewall è locale ed è di tipo software in caso di singoli PC connessi con modem.
Firewall di tipo hardware in caso di reti di PC non connessi alla WAN.
Sono vietate tutte le connessioni che non sono aderenti alla presente regola.

3.18.2.5 Misure adottate per il rischio interno

Il rischio interno è protetto:

- Per le basi dati principali: da sistemi di password su database e server
- Per le basi dati secondarie dalle protezioni standard di cui sono dotati i singoli sistemi operativi degli strumenti in uso.
- Per gli strumenti elettronici: dalle credenziali di accesso

3.18.2.6 Misure adottate per gli Amministratori di Sistema

Sono adottati sistemi per la registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) aventi caratteristiche di completezza, inalterabilità comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e sono conservate per un anno in luogo sicuro a cura del **GLP.**
L'operato degli **amministratori di sistema** è oggetto, con cadenza annuale, di un'attività di verifica da parte del **GLP**, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti

3.18.3 Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

In conformità a quanto disposto dal **punto 21 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** per ogni **supporto utilizzato per le operazioni di copia** deve essere individuato il luogo di conservazione in modo che sia convenientemente protetto dai potenziali rischi di:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto
- Accesso non autorizzato
- Trattamento non consentito

L'accesso ai supporti utilizzati per le copie dei dati è limitato per ogni banca di dati a:

- **ICSD**
- **RSPT**
- **RSTD**
- **ISM**
- **ADS**

RSTD è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati e deve indicare, utilizzando il modulo **ALL_M**, il luogo di conservazione supporti utilizzati per le copie dei dati.

3.18.4 Riutilizzo dei supporti rimovibili

In conformità a quanto disposto dal **punto 22 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** se **RSTD** decide che i supporti magnetici contenenti dati sensibili o giudiziari non siano più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto

annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.
E' compito di **RSTD** controllare e assicurarsi che in nessun caso vengano lasciate copie di **Banche di dati** contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

3.18.5 Ripristino dell'accesso ai dati in caso di danneggiamento

In conformità a quanto disposto dal **punto 23 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** la decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito di **RSTD** o di **RSPT**

La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro 7 (sette) giorni e comunque in tempi compatibili con i diritti degli interessati.
Una volta valutata la assoluta necessità di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento il **RSTD o RSPT** deve provvedere col la collaborazione di:

- **ICSD**
- **ADS**
- **Fornitore**
- **ISM**

all'operazione di ripristino dei dati.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo del **RSTD** che si può avvalere del parere di **ADS** o **ISM.**

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti deve essere presa rapidamente e in ogni caso la funzionalità deve essere ripristinata al massimo entro 7 (sette) giorni e comunque nei tempi compatibili con i diritti degli interessati.

3.19 Trattamenti effettuati da organismi sanitari e esercenti le professioni sanitarie

3.19.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 19.8 e punto 24 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003),

3.19.2 Cifratura dei dati o separazione dei dati identificativi

Il Responsabile della sicurezza dei dati personali per i trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale elencati ha stabilito di adottare le seguenti misure di sicurezza come specificato nella tabella che segue.

3.19.3 Tabella dei trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale

Descrizione del tipo di trattamento	Tipo di protezione	Tecniche adottate
SISaR CUP	O CF ● SP	O A ● B O C O D
SISaR Medicina legale	O CF ● SP	O A ● B O C O D
SISaR Anagrafica assistibili	O CF ● SP	O A ● B O C O D
SISaR Esenzione ticket	O CF ● SP	O A ● B O C O D
ALLPHARM Gestione farmacia e somministrazione diretta di farmaci	O CF ● SP	O A ● B O C O D
SISaR e ITALABCS DIANOEMA Laboratorio San Francesco	O CF ● SP	O A ● B O C O D
SISaR e METAPHORA Laboratorio Ospedale Zonchello	O CF ● SP	O A ● B O C O D

Legenda del tipo di protezione adottato:
CF Cifratura. Tutti i servizi tramite Internet il sistema di sicurezza sono basati su un protocollo TCP/IP con crittografia Secure Socket Layer (SSL) a 128 bit strong encryption emesso da Verisign Certification Authority per dare la massima garanzia che le informazioni che transitano sulla rete siano visibili unicamente dall'utente interessato. L'utilizzo di una chiave di cifratura a 128 bit garantisce il massimo livello di sicurezza a protezione del mutuo scambio di informazioni con l'utente interessato.
Il tempo necessario per decodificare tale chiave è infatti virtualmente infinito (circa 3 · 1038 possibili combinazioni).
SP Separazione architetturale tra le macchine contenenti i dati personali idonei a rivelare lo stato di salute e la vita sessuale e i server collegati ad Internet
Legenda delle tecniche di sicurezza adottate:
A E' garantita in ogni momento l'impossibilità dell'accesso non autorizzato all'infrastruttura ed ai supporti di dati.
B E' escluso l'accesso di persone non autorizzate a dati personali utilizzando un sistema di controllo delle credenziali di autenticazione.
C Le informazioni, trasmesse sono cifrate e la cifratura rispetta un livello tecnico adeguato all'attuale stato dell'arte.
D L'identificazione dell'utente interessato che ha il diritto di ricevere i dati è garantita in modo univoco.

4 Trattamenti senza l'ausilio di strumenti elettronici

4.1 Nomina e istruzioni agli incaricati

4.1.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 28 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003),

4.1.2 Misure generali

In base a quanto stabilito dall'**Art. 30 del Dlgs. n. 196 del 30 giugno 2003**, le operazioni di trattamento possono essere effettuate solo da **Incaricati del trattamento** che operano sotto la diretta autorità del **Titolare del trattamento** o, se designato, del **RSTD o del RSPT**, attenendosi alle istruzioni impartite.

4.1.3 Modalità operative

Il **RSTD** deve predisporre per ogni archivio di cui è responsabile l'elenco degli **Incaricati del trattamento** autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante per l'accesso agli archivi.
I documenti che contengono dati sensibili o giudiziari debbono essere 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.

4.2 Norme di sicurezza per gli incaricati del trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici

4.2.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 27 e punto 28 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003).

4.2.2 Modalità operative

Per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici vengono stabilite le seguenti regole che gli **Incaricati del trattamento** debbono osservare:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici , composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

- Si deve adottare ogni cautela affinché ogni persona non autorizzata, possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro e non si possono utilizzare come carta per appunti.
- Quando i documenti devono essere trasportati essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

4.3 Copie degli atti e dei documenti

In base a quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**, è fatto divieto a chiunque di:

- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **RSTD,** di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **RSTD**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

4.4 Controllo degli accessi

4.4.1 Riferimenti normativi

La Sezione è redatta in conformità a quanto disposto dal **punto 29 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003).

4.4.2 Modalità operative

L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato dai soggetti **addetti ai locali** ed è consentito, solo agli **Incaricati del trattamento** autorizzati dal **RSTD**. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, debbono essere identificate e registrate.

4.5 Verifiche Ispettive Interne

Al fine di assicurare il rispetto della Legge e le disposizioni impartite dal Titolare del Trattamento in ordine alla sicurezza dei dati personali gestiti in azienda, è istituito un piano di verifiche annuali le cui linee guida sono riportate nell' **ALL_PO02** al presente Documento Programmatico della Sicurezza.

4.5.1 Gestione delle non conformità e azioni correttive

Eventuali difformità rispetto alle disposizioni del Titolare del Trattamento rilevate durante lo svolgimento delle verifiche ispettive vengono riportate nel verbale di verifica e segnalate con uno specifico modulo di segnalazione di non conformità.

5 ORGANIZZAZIONE E PROCEDURE OPERATIVE

5.1 Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali

In questa sezione del **DPS** vengono definiti i compiti e le responsabilità per i soggetti che effettuano il trattamento.
Le istruzioni ai soggetti che effettuano i trattamenti riportate nei paragrafi e sottoparagrafi della presente sezione del **DPS** sono riportate all'interno dei singoli incarichi come allegato alla lettera di incarico. La lettera di incarico potrà contenere anche istruzioni più particolareggiate o leggermente diverse o personalizzate in virtù dei specifici trattamenti svolti dai soggetti incaricati.

5.1.1 Titolare del trattamento dei dati personali

5.1.1.1 Compiti del titolare del trattamento dei dati personali

In base a quanto definito dall'**Art. 4, punto 1, comma f) del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** il "***Titolare del trattamento*** *è 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*".
Il **Titolare del trattamento** si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)** tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.
In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)**, il **Titolare del trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del trattamento (RSTD)** anche mediante suddivisione di compiti.
I **Responsabili del trattamento** sono individuati 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.
I compiti affidati ai **Responsabili del trattamento** sono analiticamente specificati per iscritto dal **Titolare del trattamento**.
I **Responsabili del trattamento** effettuano il trattamento attenendosi alle istruzioni impartite dal **Titolare del trattamento**.

- In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili della sicurezza dei dati** che assicurino e garantiscano che vengano adottate tutte le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
- In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** il **Titolare del trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili di Specifico Trattamento dei dati**

Personali che assicurino e garantiscano che vengano adottate tutte le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.

- Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile della sicurezza dei dati**, ne assumerà tutte le responsabilità e funzioni.
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura.
- Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati Amministratori di Sistema (ADS)**.

5.1.2 Gruppo di lavoro Privacy

5.1.2.1 Compiti del Gruppo di lavoro privacy per la protezione dei dati personali

Il **Titolare del trattamento**, per esigenze organizzative, ha designato un apposito **Gruppo di lavoro privacy (GLP)** (che fino all'anno 2011 era denominato Comitato Privacy) formato da membri appartenenti alla struttura del Titolare del Trattamento.

I membri sono stati identificati e nominati con delibera. Successivamente all'adozione dell'atto deliberativo viene emesso un incarico in cui sono specificate le responsabilità che sono affidate al **GLP**.

Il **GLP** è composto da almeno 4 membri di cui uno con le funzioni di coordinatore.

Le competenze all'interno del **GLP** sono individuate in coloro che ricoprono posizioni organizzative e funzionali ed in particolare :

- Un Dirigente dell' ufficio Affari Generali
- Un Direttore Amministrativo
- Un Direttore Sanitario
- Un Responsabile Tecnico Informatico

La funzione di coordinamento del **GLP** all'atto della stesura di questo documento è svolta dalla Dott.ssa Mariangela Mameli direttore del Servizio Comunicazione in staff alla Direzione Generale.

Al **GLP** sono affidati i seguenti compiti:

- fornire supporto tecnico ai **RSTD** affinché vengano adottate le misure di sicurezza ai sensi del **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003)** tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito.
- garantire il supporto alla Direzione Aziendale nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia di protezione dei dati personali;
- provvedere alla predisposizione degli atti necessari, ai fini dell'adempimento degli oneri previsti dalla normativa suddetta;
- assicurare la propria collaborazione per la stesura del Documento Programmatico sulla Sicurezza dei dati;
- Controllare l'operato degli Amministratori di Sistema e custodire i file di log.

- Promuovere l'osservanza del regolamento aziendale sulla privacy fornendo la necessaria consulenza in ordine alle problematiche in tema di riservatezza
- Promuovere e coordinare la formazione dei dipendenti in materia di privacy
- Riportare al Titolare del Trattamento sullo stato delle misure di sicurezza e dell'adeguatezza delle stesse
- entro il 31 marzo di ogni anno raccoglie la documentazione dei moduli di registrazione aggiornati da ogni **RSTD** e ogni altra informazione necessaria per l'aggiornamento del **DPS**
- entro il 31 marzo di ogni anno compila gli elenchi basandosi sui dati trasmessi da **RSTD**
- entro il 31 marzo di ogni anno trasmette copie del DPS aggiornato a tutti i membri della lista di distribuzione riportata sul frontespizio del DPS

5.1.2.2 Verifiche ispettive interne

Il **GLP** provvede a controllare l'osservanza delle disposizioni impartite dal Titolare del Trattamento in ordine alla sicurezza dei trattamenti di dati personali anche attraverso un piano di verifiche periodiche. Le linee guida per tale attività sono riportate nell'**ALL_PO02**.

5.1.2.3 Censimento dei trattamenti

L'Azienda realizza il censimento dei dati personali e/o sensibili (anagrafe).
Il censimento contiene la rilevazione dei trattamenti dei dati suddivisi per categorie omogenee di trattamento e per strutture organizzative. Il documento viene aggiornato qualora vengano comunicati da parte del Titolare o dei Responsabili del trattamento casi di attivazione di un nuovo trattamento o cessazione di un trattamento in essere. Per tale segnalazione si utilizza il modulo TTR1 allegato a questo documento.

5.1.2.4 Nomina dei membri del gruppo di lavoro per la protezione dei dati personali

La nomina dei membri del **GLP** avviene con atto deliberativo. Il Comitato rimarrà in carica fino a nuova designazione che avverrà con formale provvedimento scritto.

5.1.3 Responsabile della sicurezza del trattamento dei dati personali

5.1.3.1 Compiti del responsabile della sicurezza del trattamento dei dati personali

In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)**, il **Titolare del trattamento**, per esigenze organizzative, ha designato più soggetti Responsabili del trattamento**.**

Il **Responsabile della sicurezza del trattamento dei dati personali** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui da parte del **Titolare del trattamento**, sono affidate le seguenti responsabilità e compiti:

- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
- Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.

- Definire e verificare periodicamente le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.
- Almeno 30 giorni prima della data del 31 marzo di ogni anno invia i dati aggiornati relativi alle registrazioni al **GLP**
- Collaborare al lavoro del **ADS** per la rilevazione e valutazione dei rischi, per l'aggiornamento del sistema di autenticazione relativo agli incaricati e del sistema di autorizzazione.

I **Responsabili della sicurezza del trattamento dei dati personali** compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di riservatezza; in particolare hanno il dovere di osservare e fare osservare le precauzioni individuate nel piano di sicurezza dei dati personali elaborato dall'Azienda.

I **Responsabili della sicurezza del trattamento dei dati personali** sono tenuti a:

- fornire al **GLP** le informazioni richieste;
- comunicare tempestivamente al **GLP** tutte le questioni rilevanti ai fini della normativa in materia di protezione dei dati personali;
- comunicare al **GLP** i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento dell'anagrafe aziendale dei trattamenti.

5.1.3.2 Nomina del Responsabile della sicurezza del trattamento dei dati personali

La nomina di ciascun **Responsabile della sicurezza del trattamento dei dati personali** deve essere effettuata dal **Titolare del trattamento** con una delibera. Successivamente all'adozione dell'atto deliberativo viene emesso un incarico in cui sono specificate le responsabilità che sono affidate al **RSTD**.
I **RSTD** sono individuati fra i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
All'interno dell'Azienda essi sono indicati in coloro che ricoprono posizioni organizzative e funzionali ed in particolare :

- Direttore Sanitario;
- Direttore Amministrativo;
- Coordinatore dei Servizi Sociali;
- Direttori di struttura complessa;
- Responsabili di struttura semplice, o altri funzionari, per i quali si rende opportuna la designazione di Responsabili del trattamento in virtù delle particolarità organizzative e funzionali delle attività di competenza.

Copia della lettera di nomina deve essere conservata a cura del **GLP** in luogo sicuro.
Il **Titolare del trattamento** deve informare ciascun **Responsabile della sicurezza del trattamento dei dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n. 196 del 30 giugno 2003)**.

Il **Titolare del trattamento** deve consegnare a ciascun **Responsabile della sicurezza del trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del **Responsabile della sicurezza del trattamento dei dati personali** è a tempo indeterminato, e decade per revoca con atto deliberativo.
La nomina del **Responsabile della sicurezza del trattamento dei dati personali** può essere revocata in qualsiasi momento dal **Titolare del trattamento** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

5.1.4 Responsabile di specifico trattamento dei dati personali

5.1.4.1 Compiti del responsabile di uno specifico trattamento di dati personali

In base a quanto stabilito dall'**Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)**, il **Titolare del trattamento**, ove necessario, per esigenze organizzative, può designare facoltativamente uno o più soggetti **Responsabili del trattamento** anche mediante suddivisione di compiti.
Il **Responsabile di uno specifico trattamento di dati personali (RSPT)** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo al quale il **Titolare del trattamento** affida il compito di gestire il trattamento dei dati personali di una o più **Banche di dati** ed ha il compito di individuare, nominare e incaricare per iscritto, gli **Incaricati del trattamento dei dati personali** del trattamento specifico di cui gli è stata assegnata la responsabilità.
I **Responsabili di uno specifico trattamento di dati personali** sono individuati 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.
Il **Responsabile di uno specifico trattamento di dati personali** ha il compito di:

- Controllare e sorvegliare che i trattamenti di dati personali e dati personali sensibili o giudiziari limitatamente alle Banche Dati e ai trattamenti di cui sono Responsabili e che sono gestiti su supporto cartaceo ma che per ragioni di praticità sono eseguiti con strumenti elettronici anche dai suoi collaboratori incaricati del trattamento, siano effettuati nei termini e nei modi stabiliti dal Codice in materia di dati personali. Di sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
- Di dare le istruzioni adeguate agli **Incaricati del trattamento** effettuato con strumenti elettronici.
- Di dare le istruzioni adeguate agli **Incaricati del trattamento** effettuato senza l'ausilio di strumenti elettronici.
- Periodicamente, e comunque almeno annualmente, di verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli **Incaricati del trattamento dei dati personali**.

5.1.4.2 Nomina dei responsabili di uno specifico trattamento di dati personali

La nomina di ciascun **Responsabile di uno specifico trattamento di dati personali** deve essere effettuata dal **Titolare del trattamento** con una delibera. Successivamente all'adozione dell'atto deliberativo viene emesso un incarico in cui sono specificate le responsabilità che sono affidate al **RSPT**.

I **RSPT** sono individuati fra i soggetti che ricoprono posizioni organizzative e funzionali ed in particolare :

- Direttore Sanitario;
- Direttore Amministrativo;
- Coordinatore dei Servizi Sociali;
- Direttori di struttura complessa;
- Responsabili di struttura semplice, o altri funzionari, per i quali si rende opportuna la designazione di Responsabili del trattamento in virtù delle particolarità organizzative e funzionali delle attività di competenza.

Copia della lettera di nomina deve essere conservata a cura del **GLP** in luogo sicuro.
Nella lettera di nomina debbono essere indicate le **Banche dati** di cui è responsabile per quanto attiene alla sicurezza e a quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
Copia della delibera e della lettera di nomina in cui sono indicate le banche dati e i trattamenti autorizzati deve essere conservata a cura del **Titolare del trattamento** in luogo sicuro.
Il **Titolare del trattamento** deve informare ciascun **Responsabile di uno specifico trattamento di dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
Il **Titolare del trattamento** deve consegnare a ciascun **Responsabile di uno specifico trattamento di dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del **Responsabile di uno specifico trattamento di dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
La nomina del **Responsabile di uno specifico trattamento di dati personali** può essere revocata in qualsiasi momento dal **Titolare del trattamento** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

5.1.5 Amministratori di Sistema (ADS)

5.1.5.1 Compiti degli Amministratori di Sistema

In conformità a quanto disposto dal **punto 1, punto 2, punto 3, punto 15, punto 16, punto 17 e punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** il **Titolare del Trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Amministratori di Sistema** (**ADS**)

L'**ADS** è la persona fisica, che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di **Banche di dati**.
L'**ADS** è anche la persona fisica che nell'esercizio delle operazioni di manutenzione e gestione dei sistemi informatici e delle basi dati può venire a conoscenza , anche accidentalmente, di dati personali pur non essendo preposti al trattamento.

E' onere del **RSTD** , in relazione all'attività svolta, individuare, tra i soggetti nominati dal **Titolare del Trattamento**, uno o più **ADS** a cui affidare la gestione e manutenzione delle banche dati e dei sistemi operativi server.

E' compito degli **ADS**:

- Rilevare in collaborazione con **RSTD** l'elenco degli archivi dei dati oggetto del trattamento, l'elenco dei trattamenti
- Attivare per tutti i trattamenti effettuati con strumenti elettronici le **Credenziali di autenticazione** assegnate agli **Incaricati del trattamento,** su indicazione del **RSTD** o del **Responsabile di uno specifico trattamento di dati personali**.
- Collaborare con **RSTD** per controllare che gli incaricati del trattamento abbiano ancora i requisiti per l'accesso alle banche dati
- Controllare i criteri di assegnazione delle credenziali di accesso alle banche dati
- In conformità a quanto disposto dal **punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso abusivo da parte di chiunque abusivamente si introduce nel sistema informatico o telematico.
- Informare il **Responsabile della sicurezza del trattamento dei dati personali** nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.
- Collaborare con **RSTD** nella stesura delle procedure per le copie di sicurezza e il ripristino dei dati
- Almeno 30 giorni prima della data del 31 marzo di ogni anno invia i dati aggiornati relativi alle registrazioni al **GLP**
- Almeno 30 giorni prima della data del 31 marzo di ogni anno redige una relazione annuale sullo stato dei rischi e su eventuali contromisure intraprese o da intraprendere (**ALL_TEC**) da trasmettere al **GLP** per allegarla al **DPS**

5.1.5.2 Nomina degli Amministratori di Sistema

Il **Titolare del Trattamento** nomina uno o più soggetti **Amministratori di Sistema** a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo e degli accessi alle **Banche di dati**.
Il **Titolare del Trattamento** deve individuare e designare gli Amministratori di Sistema tra coloro con idonee capacità ed esperienza previa valutazione delle caratteristiche di esperienza, capacità e affidabilità dei soggetti designati.
La designazione deve essere scritta e individuale e deve contenere l'elenco delle attività previste dall'**ADS** e l'ambito operativo ovvero i trattamenti, i luoghi e gli strumenti su cui il suo lavoro ha influenza.

Il **Titolare del trattamento** deve informare ciascun **Amministratore di Sistema** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore.
La nomina di uno o più **Amministratori di Sistema** deve essere effettuata con delibera. Successivamente all'adozione dell'atto deliberativo viene emesso un incarico in cui sono specificate le responsabilità che sono affidate al **ADS**.
Nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema
Copia della lettera di nomina deve essere conservata a cura del **GLP** in luogo sicuro.
Il **TTRA** deve consegnare a ciascun **ADS** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina dell'**Amministratore di Sistema** è a tempo indeterminato, e decade per revoca.
La nomina può essere revocata in qualsiasi momento dal **TTRA** senza preavviso, ed eventualmente affidata ad altro soggetto.

5.1.6 Incaricati del servizio di manutenzione (ISM)

5.1.6.1 Compiti degli incaricati del servizio di manutenzione degli strumenti elettronici

In conformità a quanto disposto dal **punto 1, punto 2, punto 3, punto 15, punto 16, punto 17 e punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** il **Titolare del Trattamento**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **incaricati del servizio di manutenzione** (**ISM**).

L'**ISM** è la persona fisica, che sovrintende alla manutenzione dei sistemi informatici e alle infrastrutture di comunicazione.

E' onere del **RSTD**, in relazione all'attività svolta, individuare, tra i soggetti nominati dal **Titolare del Trattamento**, uno o più **ISM** a cui affidare la gestione e manutenzione degli strumenti elettronici per il trattamento dei dati.

Compito del **servizio di manutenzione** è l'implementazione di tutte le operazioni tecniche necessarie ad assicurare accessi ai dati non autorizzati e l'implementazione delle misure minime conformi alle specifiche indicate nel DLgs 196/2003 e alle procedure di sicurezza interne approvate dal **Titolare del Trattamento**
I compiti dell'**ISM** sono:

- Tenere aggiornato l'elenco degli strumenti per l'eleborazione dati
- Assicurare il funzionamento degli strumenti elettronici
- Assicurare il funzionamento delle infrastrutture e degli apparati di comunicazione
- Gestire la software inventory
- Valutare i software al fine della loro certificazione interna
- Installazioni software
- Collaborare con l'ADS per assicurare la funzionalità dei sistemi informatici
- Rispondere alle richieste di intervento degli incaricati del trattamento nell'ambito delle loro competenze
- In conformità a quanto disposto dal **punto 16 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** definire l'attivazione di idonei strumenti per la protezione degli strumenti elettronici contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento. Questi strumenti debbono essere aggiornati con cadenza almeno semestrale.
- In conformità a quanto disposto dal **punto 17 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** aggiornare periodicamente (almeno una volta l'anno) i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
- In conformità a quanto disposto dal **punto 20 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso abusivo da parte di chiunque abusivamente si introduce nel sistema informatico o telematico.
- Informare il **Responsabile della sicurezza del trattamento dei dati personali** nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.
- Collaborare con **RSTD** nella stesura delle procedure per le copie di sicurezza e il ripristino dei dati

- Almeno 30 giorni prima della data del 31 marzo di ogni anno invia i dati aggiornati relativi alle registrazioni al **GLP**
- Almeno 30 giorni prima della data del 31 marzo di ogni anno redige una relazione annuale sullo stato dei rischi e su eventuali contromisure intraprese o da intraprendere (**ALL_TEC**) da trasmettere al **GLP** per allegarla al **DPS**

5.1.6.2 Nomina degli incaricati del servizio di manutenzione

Il **Titolare del Trattamento** o il **RSTD** nomina uno o più soggetti **incaricati del servizio di manutenzione** a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informatico.
La designazione deve essere scritta e individuale e deve contenere l'elenco delle attività previste e l'ambito di esecuzione del servizio.
Nel caso di servizi affidati in *outsourcing* il **GLP** conserva, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte al servizio di manutenzione
La nomina è a tempo indeterminato, e decade per revoca.
La nomina può essere revocata in qualsiasi momento senza preavviso, ed eventualmente affidata ad altro soggetto.

5.1.7 Incaricato della custodia delle copie delle credenziali

5.1.7.1 Compiti degli incaricati della custodia delle copie delle credenziali

In conformità a quanto disposto dal **punto 10 e punto 11 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)** debbono essere impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il **Titolare del trattamento** può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.
E' onere del **RSTD**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della custodia delle copie delle credenziali**.
E' compito degli **Incaricati della custodia delle copie delle credenziali**:

- Autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati personali degli **Incaricati del trattamento,** su richiesta del **Responsabile del trattamento**, avvalendosi del supporto tecnico dell'**ADS**, in conformità a quanto disposto dal **punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)**.
- Istruire gli incaricati del trattamento sull'uso delle **componenti riservata delle credenziali di autenticazione**, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia, in conformità a quanto disposto dal **punto 4 e dal punto 5 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)**.
- Assicurare che il **Codice per l'identificazione**, laddove sia stato già utilizzato, non sia assegnato ad altri **Incaricati del trattamento**, neppure in tempi diversi, in conformità a quanto disposto dal **punto 6 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)**.
- Revocare le **Credenziali di autenticazione** per l'accesso ai dati degli **Incaricati del trattamento** nel caso di mancato utilizzo per oltre 6 (sei) mesi, in conformità a quanto disposto dal **punto 7 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)**.

- Revocare tutte le **Credenziali di autenticazione** non utilizzate in caso di perdita della qualità che consentiva all'**Incaricato del trattamento** l'accesso ai dati personali, in conformità a quanto disposto dal **punto 8 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)**.
- Impartire istruzioni agli **Incaricati del trattamento** per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento, in conformità a quanto disposto dal **punto 9 del disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003)**.

In caso di prolungata assenza o impedimento di un **Incaricato del trattamento** che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, l'**Incaricato della custodia delle copie delle credenziali,** in accordo con il **Responsabile del trattamento di dati personali** può assicurare la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. Utilizzando i diritti di "amministratore di sistema", può modificare in modo forzoso la **componente riservata delle credenziali di autenticazione** dell'**Incaricato del trattamento dei dati personali** assente o impedito ad effettuare il trattamento.
2. Comunica la **componente riservata delle credenziali** di autenticazione così modificata ad un altro **Incaricato del trattamento dei dati personali** designato dal **Responsabile del trattamento di dati personali** il quale potrà utilizzarla solo temporaneamente.
3. Terminata l'assenza o l'impedimento dell'**Incaricato del trattamento** che aveva reso indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, quest'ultimo dovrà essere informato dell'intervento effettuato e dovrà modificare la propria componente riservata delle credenziali di autenticazione

5.1.7.2 Nomina degli incaricati della custodia delle copie delle credenziali

In conformità a quanto disposto dai **punti 3, 4, 5, 6, 7, 8, 9 e 10 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n. 196 del 30 giugno 2003), RSTD** nomina uno o più soggetti **Incaricati della custodia delle copie delle credenziali** a cui è conferito il compito di autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati gestiti con strumenti elettronici.
La nomina di uno o più **ICCC** deve essere effettuata con una lettera incarico in cui sono specificate le responsabilità che sono affidate al **ICCC**.
ICCC può essere individuato anche in uno degli **ADS**
Copia della lettera di nomina deve essere conservata a cura del **GLP** in luogo sicuro.
Il **RSTD** deve consegnare a ciascun **ICCC** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

Il **RSTD** deve informare gli **Incaricati della custodia delle copie delle credenziali** della responsabilità che è stata loro affidata in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** è a tempo indeterminato, e decade per revoca.
La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** può essere revocata in qualsiasi momento dal **RSTD** senza preavviso, ed essere affidata ad altro soggetto.

5.1.8 Incaricato delle copie di sicurezza delle banche dati

5.1.8.1 Compiti degli incaricati delle copie di sicurezza delle banche dati

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** il **RSTD**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati (ICSD)**.

L'**Incaricato delle copie di sicurezza delle banche dati** è la persona fisica o la persona giuridica che ha il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle **Banche di dati** personali gestite.
Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il **Responsabile della sicurezza del trattamento dei dati personali** stabilisce, con il supporto tecnico dell'**ADS** e del **Servizio di Manutenzione** la periodicità con cui debbono essere effettuate le copie di sicurezza delle **Banche di dati** trattate.
I criteri debbono essere concordati con l'**ADS** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** la frequenza con cui debbono essere effettuate le copie dei dati personali non deve superare in nessun caso i 7 (sette) giorni.
In particolare per ogni **Banca di dati** debbono essere definite le seguenti specifiche, riportato sull'apposito modello **ALL_M**:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta.
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

E' compito degli **Incaricati delle copie di sicurezza delle banche dati**:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal **Responsabile della sicurezza del trattamento dei dati personali**.
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
- Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
- Di segnalare tempestivamente all'**ADS**, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il **Responsabile della sicurezza del trattamento dei dati personali** ritenga di non nominare alcun **Incaricato delle copie di sicurezza delle banche dati**, ne assumerà tutte le responsabilità e funzioni.

5.1.8.2 Nomina degli incaricati delle copie di sicurezza delle banche dati

In conformità a quanto disposto dal **punto 18 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** il **Responsabile della sicurezza del trattamento dei dati personali**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati** a cui è conferito il compito di compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.
Il **Responsabile della sicurezza del trattamento dei dati personali** deve informare ciascun **Incaricato delle copie di sicurezza delle banche dati** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
La nomina di uno o più **Incaricati delle copie di sicurezza delle banche dati** deve essere effettuata con delibera. Successivamente all'adozione dell'atto deliberativo viene emesso un incarico in cui sono specificate le responsabilità che sono affidate al **ICSD**.
Copia della lettera di nomina deve essere conservata a cura del **GLP** in luogo sicuro.
Il **RSTD** deve consegnare a ciascun **ICSD** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

5.1.9 Incaricato del trattamento dei dati personali

5.1.9.1 Compiti degli incaricati del trattamento dei dati personali

In base a quanto stabilito dall'**Art. 30 del Dlgs. n. 196 del 30 giugno 2003**, le operazioni di trattamento possono essere effettuate solo da **Incaricati del trattamento** che operano sotto la diretta autorità del **Titolare del trattamento** o, se designato, del **RSTD** o del **RSPT**, attenendosi alle istruzioni impartite.
In base a quanto definito dall'**Art. 4, punto 1, comma h) del Dlgs. n. 196 del 30 giugno 2003**, gli *"**Incaricati del trattamento** sono persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali dal **Titolare del trattamento** o, se designato, dal **Responsabile di uno specifico trattamento di dati personali**"*.
Per i **trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici,** gli **Incaricati del trattamento dei dati personali** debbono osservare le seguenti disposizioni:

- Gli **Incaricati del trattamento dei dati personali** sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati aziendali che contengono i predetti dati personali.
- Il **trattamento dei dati personali** deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli **interessati**.
- L'**Incaricato del trattamento dei dati personali** deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni **Incaricato del trattamento dei dati personali** è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
- Gli **Incaricati del trattamento dei dati personali** che hanno ricevuto le **credenziali di autenticazione** per il trattamento dei dati personali, debbono conservare con la

massima segretezza le **componenti riservate delle credenziali di autenticazione** (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal 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.
- La **componente riservata delle credenziali di autenticazione** (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'**Incaricato del trattamento dei dati personali** deve modificare la **componente riservata delle credenziali di autenticazione** (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la **componente riservata delle credenziali di autenticazione** (parola chiave) deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.

Per i **trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici** gli **Incaricati del trattamento dei dati personali** debbono osservare le disposizioni riportate al paragrafo 4.2.2 del presente documento.

5.1.9.2 Nomina degli incaricati del trattamento dei dati personali

La nomina di ciascun **Incaricato del trattamento dei dati personali (ITDP)** deve essere effettuata dal **RSTD** o dal **RSPT** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.
Copia della lettera di nomina firmata deve essere conservata a cura del **RSTD** che ha fatto la nomina in luogo sicuro.
Il **RSTD** deve informare ciascun **Incaricato del trattamento dei dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** e dal **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n. 196 del 30 giugno 2003)**.
Il **RSTD** deve consegnare a ciascun **Incaricato del trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
Gli **Incaricati del trattamento dei dati personali** devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli **ITDP** deve essere assegnata una **credenziale di autenticazione**.
Agli **Incaricati del trattamento dei dati personali** è prescritto di adottare le necessarie cautele per assicurare la segretezza della **componente riservata della credenziale di autenticazione** e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.
La nomina dell'**Incaricato del trattamento dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.
La nomina dell'**Incaricato del trattamento dei dati personali** può essere revocata in qualsiasi momento dal **RSTD**, senza preavviso, ed eventualmente può essere affidata ad altro soggetto.

La nomina di uno o più **Incaricati del trattamento dei dati personali** deve essere effettuata in forma scritta. Successivamente all'adozione dell'atto deliberativo viene emesso un incarico in cui sono specificate le responsabilità che sono affidate agli incaricati del trattamento dei dati personali.

Il **RSTD** deve consegnare a ciascun **ITDP** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
Il fac-simile del contenuto della delibera per l'emissione dell'incarico del trattamento dei dati personali è l'allegato **LI_IDT2**.

La designazione può avvenire anche attraverso la documentata assegnazione ad una unità per la quale è stato individuato, per iscritto, l'ambito del trattamento consentito agli addetti dell'unità medesima (incaricati per ufficio/reparto).
L'individuazione dell'ambito dei trattamenti consentiti all'interno di un ufficio/reparto avviene attraverso il modello fac-simile allegato **LI_IDT3** in cui sono specificati:

- La sede operativa in cui avviene il trattamento
- L'ufficio/reparto
- Le banche dati
- I permessi per ogni banca dati
- I tipi di dati trattati
- Le finalità del trattamento
- Il contenuto della banca dati

Il modello contiene anche le istruzioni per gli incaricati **al trattamento dei dati personali**.

RSDT può redigere un elenco di incaricati del trattamento dei dati personali per classi omogenee di incarico. Allo stesso modo possono essere emessi anche incarichi per unità o reparto in cui sono individuati per iscrito l'ambito dei trattamenti consentiti. In questo caso, come previsto all'art. 30 del D.Lgs 196/2003 comma 2, l'incaricato del trattamento si considera designato con la documentata preposizione all'unità o reparto.

Anche in caso di designazione per unità/reparto degli incaricati, le istruzioni per il trattamento vanno comunque consegnate per iscritto ad ogni incaricato.

RSDT provvederà a conservare e tenere aggiornato un registro di consegna delle istruzioni agli incaricati controfirmato da questi ultimi.

Copia della dell'incarico del trattamento dei dati personali per unità/reparto deve essere conservata a cura del **RSDT** in luogo sicuro.
Il **RSTD** deve provvedere a comunicare a ciascun **ITDP** alle sue dipendenze tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

L'incarico personale è di rango superiore rispetto all'incarico dato per unità/reparto per cui in presenza di ridondanze avrà priorità l'incarico ad personam.

5.2 Misure di tutela e garanzia

5.2.1 Descrizione degli interventi effettuati da soggetti esterni

In conformità al **punto 25 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n. 196 del 30 giugno 2003)** nel caso in cui ci si avvalga di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento hardware e/o software degli strumenti elettronici e alla eventuale riparazione, aggiornamento o sostituzione, il **Responsabile della sicurezza del trattamento dei dati personali**, deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)**.

6 Diritti dell'interessato

6.1 Comunicazioni all'interessato

In conformità **all'art. 84 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** "*I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare*".

"*Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a):*

[incapacità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;]

L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati."

6.2 Finalità di rilevante interesse pubblico (Artt. 85 e 86 DLgs 196/03)

6.2.1 Compiti del servizio sanitario nazionale (Art. 85 DLgs 196/03)

1. Fuori dei casi di cui al comma 2, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità che rientrano nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative alle seguenti attività:
a) attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale;
b) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
c) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
d) attività certificatorie;
e) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;
f) le attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;
g) instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.

2. Il comma 1 non si applica ai trattamenti di dati idonei a rivelare lo stato di salute effettuati da esercenti le professioni sanitarie o da organismi sanitari pubblici per finalità di tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività, per i quali si osservano le disposizioni relative al consenso dell'interessato o all'autorizzazione del Garante ai sensi dell'articolo 76.

3. All'identificazione dei tipi di dati idonei a rivelare lo stato di salute e di operazioni su essi eseguibili è assicurata ampia pubblicità, anche tramite affissione di una copia o di una guida illustrativa presso ciascuna azienda sanitaria e presso gli studi dei medici di medicina generale e dei pediatri di libera scelta.

4. Il trattamento di dati identificativi dell'interessato è lecito da parte dei soli soggetti che perseguono direttamente le finalità di cui al comma 1. L'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività di cui al medesimo comma, secondo il principio dell'indispensabilità dei dati di volta in volta trattati.

6.2.2 Art. 86 DLgs. 196/03

(Altre finalità di rilevante interesse pubblico)

1. Fuori dei casi di cui agli articoli 76 e 85, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità, perseguite mediante trattamento di dati sensibili e giudiziari, relative alle attività amministrative correlate all'applicazione della disciplina in materia di:
a) tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza;
b) stupefacenti e sostanze psicotrope, con particolare riferimento a quelle svolte al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti, gli interventi anche di tipo preventivo previsti dalle leggi e l'applicazione delle misure amministrative previste;
c) assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di:
1) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni;
2) curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge;
3) realizzare comunità-alloggio e centri socio riabilitativi;
4) curare la tenuta degli albi degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore.

2. Ai trattamenti di cui al presente articolo si applicano le disposizioni di cui all'articolo 85, comma 4.

6.3 Dati Genetici (Art. 90 DLgs. 196/03)

1. Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità.

2. L'autorizzazione di cui al comma 1 individua anche gli ulteriori elementi da includere nell'informativa ai sensi dell'articolo 13, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi.

3. Il donatore di midollo osseo, ai sensi della legge 6 marzo 2001, n. 52, ha il diritto e il dovere di mantenere l'anonimato sia nei confronti del ricevente sia nei confronti di terzi.

6.4 Disposizioni Varie (Artt. 91, 92, 93, 94 DLgs. 196/03)

6.4.1 Dati trattati mediante carte

1. Il trattamento in ogni forma di dati idonei a rivelare lo stato di salute o la vita sessuale eventualmente registrati su carte anche non elettroniche, compresa la carta nazionale dei servizi, o trattati mediante le medesime carte è consentito se necessario ai sensi dell'articolo 3, nell'osservanza di misure ed accorgimenti prescritti dal Garante nei modi di cui all'articolo 17.

6.4.2 Cartelle cliniche

1. Nei casi in cui organismi sanitari pubblici e privati redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

6.4.3 Certificato di assistenza al parto

1. Ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Si osservano, altresì, le disposizioni dell'articolo 109.

2. Il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata avvalendosi della facoltà di cui all'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento.

3. Durante il periodo di cui al comma 2 la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

6.4.4 Banche dati, registri e schedari in ambito sanitario

1. Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, è effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso:

a) il registro nazionale dei casi di mesotelioma asbesto-correlati istituito presso l'Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), di cui all'articolo 1 del decreto del Presidente del Consiglio dei ministri 10 dicembre 2002, n. 308;
b) la banca di dati in materia di sorveglianza della malattia di Creutzfeldt-Jakob o delle varianti e sindromi ad essa correlate, di cui al decreto del Ministro della salute in data 21 dicembre 2001, pubblicato nella *Gazzetta Ufficiale* n. 8 del 10 gennaio 2002;
c) il registro nazionale delle malattie rare di cui all'articolo 3 del decreto del Ministro della sanità in data 18 maggio 2001, n. 279;
d) i registri dei donatori di midollo osseo istituiti in applicazione della legge 6 marzo 2001, n. 52;
e) gli schedari dei donatori di sangue di cui all'articolo 15 del decreto del Ministro della sanità in data 26 gennaio 2001, pubblicato nella *Gazzetta Ufficiale* n. 78 del 3 aprile 2001.

6.5 Diritto di accesso ai dati personali

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

6.6 Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al Titolare o al Responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.
2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:
a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;

b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.
3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.
4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

6.7 Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.
2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.
3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.
5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

6.8 Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:
a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.
2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.
3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.
4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.
5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.
6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.
7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.
8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.
9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

7 SCADENZARIO

7.1 Principi Generali

- Trattare i dati personali secondo i principi indicati dalla legge;
- Controllare la pertinenza e non eccedenza dei dati trattati rispetto alle finalità della raccolta (art.11);
- Controllare l'esattezza dei dati ed eventualmente, qualora si renda necessario, provvedere al loro aggiornamento (art.11);
- Conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi della raccolta (art.11); superato tale termine, provvedere alla cancellazione del dato, ovvero alla sua trasformazione in forma anonima;
- Individuare le figure attive del trattamento: il *Titolare*, l'*incaricato*, il *Responsabile* (figura facoltativa), l'*amministratore di sistema*, il *soggetto preposto alla custodia delle parole-chiave*.
  Nominare tali soggetti in forma scritta, fornendo le relative istruzioni.
- Rendere ai soggetti interessati l'informativa di cui all'articolo 13, 77,78,79,80 anche in forma orale;
- Acquisire il consenso per il trattamento dei dati comuni e sensibili dell'interessato, (art. 81);
- Rispondere alle richieste dell'interessato (Art. 7) entro massimo quindici giorni.

7.2 MISURE MINIME

- Annualmente, aggiornare l'individuazione dell'ambito di trattamento consentito ai singoli incaricati, ove variato, anche parzialmente;
- Annualmente, e precisamente entro il 31 marzo di ogni anno, redigere il Documento programmatico sulla sicurezza di cui all'art.19, Allegato B
- Aggiornare con cadenza almeno semestrale gli strumenti elettronici utilizzati al fine di proteggere i dati dal rischio di intrusione e dal rischio derivante da virus informatici (art. 16, Allegato B);
- Aggiornare con cadenza almeno semestrale i programmi per computer volti a prevenire la vulnerabilità di strumenti elettronici ed a prevenirne i difetti (art. 17, Allegato B);
- Controllare periodicamente e assicurarsi che il salvataggio dei dati sia effettuato almeno settimanalmente;
- Annualmente, programmare interventi di formazione per gli incaricati del trattamento
- Dare comunicazione al Garante circa la necessità di diffondere dati personali o comunicarli ad altri soggetti pubblici, quando ciò non sia previsto dalla legge o da un regolamento, qualora ciò risulti comunque necessario per lo svolgimento delle funzioni istituzionali (Art. 19, D.Lgs. 196/2003); nei casi previsti dall'art. 39, effettuare le comunicazioni al Garante entro il 30 giugno 2004.
- Controllare l'esistenza di norme di legge o di regolamento prima di effettuare comunicazione o diffusione di dati a soggetti privati o ad enti pubblici economici.
- Identificare e rendere pubblici i tipi di dati e le operazioni effettuabili sui dati sensibili, nel caso in cui una norma di legge specifichi solo le rilevanti finalità di interesse pubblico da seguire (art.20).

7.3 NOTIFICAZIONE

- Le notificazioni devono essere effettuate prima dell'inizio del **nuovo** trattamento (qualunque esso sia, manuale o automatizzato), se si rientra in una delle ipotesi previste dall'art. 37 del Codice.

7.4 PRINCIPALI ADEMPIMENTI PERIODICI

Oltre ai principi generali appena enunciati, il D.Lgs. 196/2003 impone una serie di verifiche e controlli da effettuare con cadenza periodica, o per espressa previsione normativa, o perché necessario procedere ad alcune modifiche ogniqualvolta muti uno degli elementi essenziali dell'organizzazione aziendale.

7.4.1 1° gennaio di ogni anno

(si tratta degli adempimenti per i quali il Codice prevede una cadenza almeno annuale):

- Aggiornare l'individuazione dell'ambito di trattamento consentito ai singoli incaricati, ove variato, anche parzialmente;
- Verificare la sussistenza delle condizioni per la conservazione delle autorizzazioni per l'accesso ai dati particolari per gli incaricati;
- Fornire istruzioni organizzative e tecniche affinché il salvataggio dei dati sia effettuato settimanalmente;
- Programmare interventi di formazione per gli incaricati del trattamento.

7.4.2 1°gennaio-1°luglio di ogni anno

(adempimenti a cadenza semestrale):

- Aggiornare i software antivirus, per tutti i tipi di dati (art. 16, Allegato B);
- Provvedere all'aggiornamento delle "*patch*" dei programmi per computer, (art. 17, Allegato B);

7.4.2.1 Criteri adottati nel DPS

L'aggiornamento dei software e delle patch è stabilito con un programma quadrimestrale:

- dal 1 al 30 gennaio,
- dal 1 al 30 maggio
- dal 1 al 30 settembre

7.4.3 31 marzo di ogni anno:

- Aggiornare il **Documento programmatico sulla sicurezza.**

  All'interno del documento programmatico per la sicurezza, è previsto un **PIANO DI FORMAZIONE** per gli incaricati, che dovrà pertanto essere rivisto annualmente. Il piano impone che siano fatte previsioni effettive sui tempi di formazione e sulle strutture che gestiranno tali attività, nell'arco dell'anno. La formazione è programmata al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o

introduzione di nuovi significativi strumenti, rilevanti per il trattamento dei dati personali.

Quanto ai Responsabili, questi devono essere scelti tra persone dotate della necessaria esperienza, capacità, affidabilità: è, quindi, opportuno che la loro formazione sia più specifica rispetto a quella data agli incaricati, onde evitare il rischio di nomine invalide.

Il Documento programmatico sulla sicurezza deve essere effettuato, in sede di prima applicazione del Codice, entro il 31 marzo 2006.

7.5 ALTRI ADEMPIMENTI

In tutti i casi che seguono è necessario procedere a verifiche costanti (il legislatore non indica un periodo minimo di revisione, ma punisce dichiarazioni eventualmente difformi dalla realtà):

7.5.1 NOTIFICA

Sarà necessario provvedere alla modifica della notificazione effettuata al Garante tutte le volte in cui cambi uno degli elementi in essa contenuti

7.5.2 INFORMATIVE

E' necessario distribuire nuove informative, o comunicare i mutamenti intervenuti, tutte le volte in cui cambi uno degli elementi descritti dall'art. 13 del Codice:

a. le finalità e le modalità del trattamento cui sono destinati i dati;
b. la natura obbligatoria o facoltativa del conferimento dei dati;
c. le conseguenze di un eventuale rifiuto di rispondere;
d. i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
e. il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del Titolare.

Non c'è obbligo di modificare l'informativa qualora cambino i Responsabili, che siano stati indicati nell'informativa solo in base alla qualifica rivestita; può anche essere indicato solo il luogo dove è conservato l'elenco completo dei Responsabili del trattamento, ovvero il modo per accedervi. E' comunque necessario indicare nome e dati di almeno un Responsabile, se nominato.

7.5.3 QUALITA' DEI DATI ex art. 11

Il Titolare deve curare che il trattamento dei dati avvenga sempre nel rispetto dei principi dettati dall'art.11 del Codice; dunque, **occorre verificare costantemente**:

a. che i dati siano trattati in modo lecito e secondo correttezza;
b. che siano raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
c. che siano esatti e, se necessario, aggiornati;
d. pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e. conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

7.5.4 CONSENSO

E' necessario, in generale, procedere alla verifica dell'esistenza del consenso ogniqualvolta il trattamento sia effettuato per scopi diversi da quelli per cui il consenso era stato inizialmente prestato, nonché tutte le volte in cui i dati debbano essere comunicati a soggetti terzi, o diffusi ad un numero di persone indeterminato.

8 Regolamento Aziendale

Il presente capitolo contiene disposizioni attuative del D.lgs. 196/03 (Codice in materia di protezione dei dati personali) nell'ambito delle strutture dell'Azienda ASL N. 3 di Nuoro, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda medesima.

L'Azienda adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'Azienda adotta altresì le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'art. 7 del D.lgs. 196/03.

8.1 Informativa all'interessato

L'informativa è l'elemento propedeutico al trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività di trattamento che vengono poste in essere.

L'informativa è sempre dovuta a prescindere dall'obbligo di acquisizione del consenso.
Essa deve contenere gli elementi tassativamente indicati dall'art. 13 del D.lgs. 196/03 e più specificatamente:

- le finalità e le modalità con le quali vengono trattati i dati;
- l'obbligatorietà o meno del conferimento dei dati;
- le conseguenze di un eventuale rifiuto a fornire i dati;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'articolo successivo;
- gli estremi identificativi del Titolare e del Responsabile al trattamento;
- La predetta informativa può essere resa anche tramite affissione di appositi manifesti nei locali di accesso all'utenza, secondo procedure e attraverso modelli concordati con il **GLP**

8.2 Consenso al trattamento dei dati

L'Azienda ASL N. 3 di Nuoro tratta i dati idonei a rivelare lo stato di salute:

a) con il consenso dell'interessato se il trattamento riguarda dati ed operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;

b) anche senza il consenso dell'interessato, ma previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

Nell'ambito di attività istituzionali c.d. "amministrative", invece, non vi è la necessità di richiedere il consenso dell'interessato, fermo restando il rispetto dell'obbligo dell'informativa.

Con Deliberazione n. in esecuzione dell'accordo tra Azienda ASL N.3 di Nuoro ed Ordine Provinciale dei Medici Chirurghi ed Odontoiatri di Nuoro, i Medici di Medicina Generale e i Pediatri di Libera Scelta sono delegati ad informare i propri assistiti e ad acquisire il relativo consenso al trattamento dei dati personali per conto dell'Azienda ASL N.3 di Nuoro.

Rimane salva la facoltà dell'Azienda di procedere al rilascio dell'informativa ed all'acquisizione del consenso in modo autonomo presso le proprie strutture / servizi.

8.3 Criteri per l'esecuzione del trattamento dei dati personali

Il trattamento dei dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato.
Oggetto del trattamento devono essere i soli dati essenziali per lo svolgimento delle attività istituzionali.
I dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per i quali sono raccolti e trattati.
Nei trattamenti è autorizzata solo l'esecuzione delle operazioni strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.
E' compito dei **Responsabili della Sicurezza del trattamento dei dati Personali** verificare periodicamente la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisca di propria iniziativa.
I dati che, anche a seguito di verifiche, risultassero eccedenti, non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
I trattamenti di dati effettuati impiegando banche dati di più titolari diversi dall'Azienda ASL N. 3 di Nuoro (interconnessione di banche dati), sono utilizzati nelle sole ipotesi previste da espressa disposizione di legge.
I dati contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di mezzi elettronici o comunque automatizzati, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altri sistemi che, considerato il numero e la natura dei dati trattati, permettono di identificare gli interessati solo in caso di necessità
I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo e in modo da risalire ai dati identificativi dell'interessato solo in caso di necessità.
In ogni caso devono essere adottate misure tecniche tali da garantire che i dati personali o sensibili siano accessibili ai soli incaricati di trattamento e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

8.4 Operazioni eseguibili

Si possono svolgere unicamente le operazioni di trattamento strettamente necessarie al perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi esercitati anche su richiesta di altri soggetti.
Le operazioni di raffronto tra dati sono effettuati solo con l'indicazione scritta dei motivi.

Resta fermo il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

8.5 Misure per il rispetto dei diritti dell'interessato

In conformità **all'art. 83 del Codice in materia di protezione dei dati personali (Dlgs. n. 196 del 30 giugno 2003)** sono adottate idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.

8.5.1 Chiamate nelle sale d'attesa

Nelle sale di attesa all'interno delle strutture sanitarie, la chiamata dei nominativi in lista d'attesa avviene attraverso il riferimento ad un numero d'ordine senza mai fare riferimento al nome dell'interessato allo scopo di preservare la Sua identità e prevenire nei confronti di estranei un esplicita correlazione tra il nome dell'interessato e reparti o strutture indicativa dell'esistenza di un particolare stato di salute.

8.5.1.1 Modalità operative

Ad ogni nominativo viene assegnato un numero progressivo che in alcuni casi può determinare anche l'ordine di chiamata. L'assegnazione del numero progressivo può avvenire con sistemi di gestione delle code d'attesa, bigliettini prenumerati, o, se previsto generato dal sistema informatico. La chiamata, che può avvenire anche con l'uso di apparati vocali, avviene pronunciando il numero assegnato.

8.5.2 Distanze di cortesia

Strisce di delimitazione, avvisi scritti e ambienti separati sono utilizzati al fine di mantenere condizioni tali da consentire la riservatezza delle comunicazioni e prevenire l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute durante i colloqui.

8.5.3 Prestazioni sanitarie e documenti di anamnesi

Le prestazioni sanitarie e la documentazione di anamnesi vengono sempre trattate in locali e ambienti in cui è garantita la riservatezza dell'interessato e comunque mai in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti.

8.5.4 Rispetto e tutela della dignità dell'interessato

Viene sempre rispettata la dignità dell'interessato in occasione delle prestazioni mediche e in ogni altra operazione di trattamento dei dati.
La tutela della dignità della persona deve essere sempre garantita. In particolare, riguardo a fasce deboli (disabili, minori, anziani), ma anche a pazienti sottoposti a trattamenti medici invasivi o per i quali è doverosa una particolare attenzione (es. interruzione della gravidanza). Nei reparti di rianimazione sono adottati accorgimenti anche provvisori (es. paraventi) per delimitare la visibilità dell'interessato, durante l'orario di visita, ai soli familiari e conoscenti.

8.5.5 Notizie sullo stato di salute

Prima di fornire qualunque notizia (anche telefonica) sullo stato di salute degli interessati ci si deve assicurare che il terzo sia legittimato. A tal fine è istituito un registro delle persone

legittimate che devono essere preventivamente identificate prima di fornire qualsiasi tipo di notizia riguardante lo stato di salute dell'interessato.

8.5.6 Notizie al pronto soccorso

L'organismo sanitario può dare notizia, anche per telefono, sul passaggio o sulla presenza di una persona al pronto soccorso, ma solo ai terzi legittimati, come (parenti, familiari, conviventi). L'interessato, se cosciente e capace, viene preventivamente informato (es. all'accettazione) che può decidere a quali soggetti può essere comunicata la sua presenza al pronto soccorso.

8.5.7 Riservatezza nei colloqui

Quando prescrive medicine o rilascia certificati, il personale sanitario evita che le informazioni sulla salute dell'interessato possano essere conosciute da terzi.

8.5.8 Informazioni sulla degenza

In occasione di richieste da parte di terzi legittimati sulla dislocazione degli interessati nell'ambito dei reparti ci si assicura preventivamente che l'interessato non abbia manifestato eventuali legittime contrarietà.
Le strutture sanitarie possono dare informazioni sulla presenza dei degenti nei reparti, ma solo a terzi legittimati (familiari, conoscenti, personale volontario). Anche qui l'interessato, se cosciente e capace, deve essere informato al momento del ricovero e poter decidere quali soggetti possono venire a conoscenza del ricovero e del reparto di degenza.

8.5.9 Informazioni sullo stato di salute

Si possono dare informazioni sullo stato di salute a soggetti diversi dall'interessato quando questi abbia manifestato uno specifico consenso. Tale consenso può essere dato da un familiare in caso di impossibilità fisica o incapacità dell'interessato o, valutato il caso, anche da altre persone legittimate a farlo, come familiari, conviventi o persone in stretta relazione con l'interessato stesso.
I soggetti terzi che hanno accesso alle strutture sanitarie (es. associazioni di volontariato), per poter conoscere informazioni sulle persone in relazione a prestazioni e cure devono rispettare tutte le regole e le garanzie previste dalle strutture sanitarie per il proprio personale, come ad esempio vincoli di riservatezza, possibilità e modalità di approccio ai degenti.

8.5.10 Ritiro di analisi

I referti diagnostici, i risultati delle analisi e i certificati rilasciati dai laboratori di analisi o dagli altri organismi sanitari possono essere ritirati anche da persone diverse dai diretti interessati purché munite di delega scritta e con consegna in busta chiusa.

8.5.11 Formazione del personale

Il personale viene informato attraverso la distribuzione di opuscoli informativi allo scopo di prevenire nei confronti di estranei un esplicita correlazione tra l'interessato e reparti o strutture indicativa dell'esistenza di un particolare stato di salute.
Annualmente sono organizzate sessioni formative in materia di privacy per i responsabili.
La formazione è programmata al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o introduzione di nuovi significativi strumenti, rilevanti per il trattamento dei dati personali.

8.5.12 Segreto professionale

Tutto il personale è tenuto al segreto professionale, anche coloro che per Legge non vi sono tenuti, e sono informati sulle regole di condotta da tenere attraverso opuscoli informativi.

8.6 Comunicazione dei dati

La comunicazione di dati personali da parte dell'Azienda ASL N. 3 di Nuoro ad altri soggetti pubblici è ammessa solo quando sia prevista da una norma di legge o di regolamento (art. 19, comma 2, D.lgs. 196/03). In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di 45 giorni dalla data di comunicazione obbligatoriamente preventiva al Garante e non sia stata adottata dall'Autorità diversa determinazione (art. 39, comma 2, D.lgs. 196/03).
La comunicazione da parte dell'Azienda ASL N. 3 di Nuoro di dati personali a privati e la diffusione sono ammesse unicamente quando siano previste da una norma di legge o di regolamento (art. 19, comma 3 D.lgs. 196/03).
I dati idonei a rivelare lo stato di salute non possono essere diffusi (art. 22, comma 8 D.lgs. 196/03).

8.7 Responsabili della sicurezza dei dati personali

L'elenco completo delle nomine è disponibile presso l'Ufficio del Coordinatore del **GLP.**

8.8 Diritto di accesso alla documentazione amministrativa

L' accesso ai documenti amministrativi deve avvenire in conformità all'art. 24 della Legge 7 agosto 1990 n. 241.

8.9 Diritto di accesso alla documentazione sanitaria

Ai sensi dell'art. 92 d.lgs. 196/03, eventuali richieste di presa visione o di rilascio di copia della cartella clinica e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Le richieste di accesso alle cartelle cliniche ospedaliere di un terzo sono valutate dal **Titolare del Trattamento**, che ne ha la responsabilità, applicando i criteri enunciati.

Ai fini del bilanciamento degli interessi potrà essere chiesto parere al **GLP**.

Le modalità in ordine alle richieste di rilascio di copie della documentazione sanitaria sono oggetto di apposita regolamentazione.

Tutta la documentazione sanitaria (non solo la cartella clinica) può essere ritirata anche da persona diversa dal diretto interessato, purché sulla base di una delega scritta e mediante consegna dei documenti in busta chiusa.

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo attraverso le forme previste dall'art. 84 del d.lgs. 196/03.