# ARNAS " GARIBALDI" DI CATANIA

**Direttore Generale**

**Dott. Giorgio Giulio Santonocito**

# AGGIORNAMENTO

# DOCUMENTO RIEPILOGATIVO

***IN MATERIA DI MISURE MINIME DI SICUREZZA***

***del***

***CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI***

**(Decreto legislativo 30 giugno 2003, n. 196)**

**Premessa**

**1. Gli obblighi in materia di trattamento dei dati personali**

Il Decreto Legislativo 30 giugno 2003, n.196 garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti delle persone fisiche, con particolare riferimento alla riservatezza e alla identità delle persone, definendo alcuni principi generali in materia di protezione dei dati personali e sensibili e precisamente:

– principio di necessità nel trattamento dei dati, di cui all'articolo 3, relativamente alla necessità di far sì che i sistemi informativi e i programmi informatici siano configurati per ridurre al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità;

– la trasparenza, di cui all'articolo 13, relativamente all'obbligo per il titolare del trattamento dati di manifestare all'esterno e far conoscere una serie di elementi caratterizzanti la propria attività di trattamento. Da qui, l'esigenza di provvedere alla notifica al Garante, nei casi previsti dal decreto all'art. 37 del "codice della privacy" e quella di fornire l'informativa all'interessato;

– l'obbligo di adozione delle misure minime di sicurezza, di cui agli articoli dal 31 al 36 e all'allegato B, relativamente alle modalità di protezione dei dati personali, che prevede, tra l'altro, l'obbligo di valutazione in process delle stesse e il relativo continuo adattamento anche in base alle conoscenze acquisite con il progredire delle tecnologie, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il documento programmatico sulla sicurezza (D.P.S.), di cui all'articolo 34 del codice, viene indicato come una delle sopracitate misure minime di cui si deve dotare ogni gestore di dati personali. Tale documento descrive lo standard di sicurezza dei dati trattati detenuti dall'Ente ed indica gli strumenti chiave per gestire al meglio tutti gli aspetti relativi alla sicurezza informatica dei dati e delle risorse di elaborazione che necessitano di protezione.

Il decreto legge del 9 febbraio 2012, n. 5, "Disposizioni urgenti in materia di semplificazione e di sviluppo", è intervenuto nelle disposizioni del codice in materia di trattamento dei dati personali ed in particolare negli obblighi relativi al sopracitato D.P.S., anche con lo scopo di assicurare,

nell'attuale eccezionale situazione di crisi internazionale e nel rispetto del principio di equità, una riduzione degli oneri amministrativi per i cittadini e le imprese e la crescita, il sostegno e l'impulso al sistema produttivo del Paese.

In particolare, l'articolo 45 del decreto semplificazioni, intervenendo sull'articolo 34 del codice della privacy ha soppresso la lettera g) del comma 1 e, abrogando il comma 1-bis, ha eliminato l'obbligo di aggiornamento del documento programmatico sulla sicurezza.

Il sopra citato decreto, tuttavia, ha abrogato esclusivamente la redazione e l'aggiornamento del DPS, mantenendo invece e correttamente inalterati tutti i restanti obblighi previsti dal Codice della Privacy, che rimangono pertanto in vigore. Tra questi l'obbligo dell'adozione di adeguate misure minime di sicurezza.

Rimane, in particolare, obbligatorio adottare:

- le altre misure del Codice e del relativo all. B;
- le diverse designazioni e nomine (incaricati, responsabili interni e responsabili esterni);
- gli obblighi di informativa ed eventuale consenso al trattamento (art. 13);
- l'adozione delle misure previste da particolari provvedimenti generali dell'autorità Garante (provvedimento video sorveglianza, uso di Internet e mail nei luoghi di lavoro ecc.);
- previsioni specifiche previste nelle autorizzazioni generali o in provvedimenti simili (autorizzazione al trattamento di dati genetici).

Chiarito, quindi, che l'eliminazione del D.P.S. non equivale a eliminare le misure minime di sicurezza, è necessario prevedere un documento che elenchi, riassuma e pianifichi, anche in relazione ai rischi, le misure di sicurezza in materia di trattamento dei dati e, inoltre, tenga traccia delle modifiche e delle evoluzioni a seconda dei dati trattati e degli strumenti utilizzati.

Il suddetto documento, in sostanza, deve "misurare" la sicurezza fisica, logica, organizzativa raggiunta dall'Ente nel trattamento dei dati personali e comprovare la conformità delle misure adottate alla normativa vigente.

E' quindi opportuno redigere un **"Documento Riepilogativo"** speculare all'ex DPS, ancorchè privo dei vincoli costrittivi del punto 19 all. B Codice Privacy, provvedendo a predisporre:

2. i criteri di autenticazione ed autorizzazione informatica;
3. la gestione delle credenziali di autenticazione;
4. utilizzazione di un sistema di autorizzazione;
5. l'aggiornamento periodico degli incarichi conferiti ai singoli addetti al trattamento dei dati personali;

6. una più forte, precisa e puntuale attuazione di policy aziendale per l'utilizzo e protezione degli strumenti elettronici e dei dati rispetto ai trattamenti;
7. l'adozione di procedure per la custodia di copie di backup;
8. una solida politica di disaster ricovery per il ripristino della disponibilità dei dati e dei sistemi.
9. l'autorizzazione formale a gestire dati per i collaboratori esterni;
10. la predisposizione di Informative per gli interessati, dipendenti e fornitori;
11. la predisposizione del consenso al trattamento dei dati;
12. la verifica di pertinenza, esattezza, aggiornamento e rispetto alle finalità di raccolta dei dati gestiti;
13. un'idonea regolamentazione, in forma specifica, per particolari modalità del trattamento dei dati, (come ad esempio la video sorveglianza )

## 2. Scopo e obiettivi

Il presente Documento Riepilogativo sulla sicurezza, si propone quindi di:

– descrivere le misure adottate e pianificate al fine di garantire la riservatezza, l'integrità, la disponibilità e l'autenticità dei dati trattati;
– contenere informazioni atte ad illustrare quanto realizzato e predisposto in materia di sicurezza;
– evidenziare eventuali nuove esigenze o la necessità di adeguamenti, anche al fine di garantire:

- un sistema aggiornato di criteri di autenticazione ed autorizzazione informatica;
- la redazione di idonee informative per gli interessati, i dipendenti e i fornitori;
- la predisposizione aggiornata del consenso al trattamento dati;
- le nomine degli incarichi al trattamento dei dati personali nonché l'aggiornamento periodico delle stesse;
- l'adozione delle misure previste da particolari provvedimenti generali dell'Autorità Garante;
- la gestione di una privacy policy puntuale e precisa per l'utilizzo e la protezione degli strumenti elettronici e dei dati rispetto ai trattamenti;
- la gestione di un politica di disaster ricovery per il ripristino delle disponibilità dei dati e dei sistemi.

## 3. Fonti normative

Le disposizioni di legge principali concernenti la corretta gestione di sistemi informatici sono:

– decreto legislativo del 30 giugno 2003, n.196, Codice in materia di protezione dei dati personali e suo Disciplinare Tecnico, allegato B;
– decreto legge del 9 febbraio 2012, n. 5, recante "Disposizioni urgenti in materia di semplificazione e sviluppo".

## 4. Misure generali

### Elenco dei trattamenti

L'individuazione dei trattamenti effettuati dall'ARNAS Garibaldi di Catania, è avvenuta utilizzando la ricognizione generale di tutti i trattamenti di dati, ordinari, sensibili, genetici e giudiziari, effettuata presso tutte le Unità Operative e Servizi, così come previsto dal Regolamento Aziendale Privacy.

### Responsabili del trattamento dei dati

Con Deliberazione n. 24 del 20 gennaio 2015 il Direttore Generale, dati i mutati assetti organizzativi, ha aggiornato l'elenco dei Responsabili del trattamento individuando i nuovi Responsabili.
A Ciascun nuovo Responsabile del trattamento dei dati identificato riceverà copia della Delibera in oggetto e lettera di incarico a firma del Direttore Generale.
Copia della lettera, controfirmata dall'interessato, viene conservata a cura della Segreteria della Commissione per il Diritto alla Riservatezza dei dati.
Il nuovo elenco dei Responsabili interni del trattamento verrà pubblicato sul sito web aziendale

### Trattamenti affidati all'esterno

L'ARNAS Garibaldi, in qualità di Titolare dei dati, sta procedendo alla nuova individuazione dei Responsabili esterni del Trattamento dei dati delle Ditte esterne che possono trattare dati sensibili per procedere alla loro nomina.
Il nuovo elenco dei Responsabili esterni del trattamento verrà pubblicato sul sito web aziendale

### Risorse da tutelare

Le risorse da tutelare, al fine di adottare le misure di sicurezza, sono suddivise in: ambiente fisico, hardware, software, accesso ai dati.

Vengono presi in considerazione, per:

– ambiente fisico: edifici; locali di ubicazione degli archivi informatizzati, locali di conservazione dei dati cartacei;
– hardware: strumenti utilizzati
– software: software utilizzati
– accesso ai dati: interconnessione e stazioni di lavoro per l'accesso

## 5. Misure minime in essere e da adottare per la prevenzione dei rischi

Scopo del presente paragrafo è descrivere le **misure adottate** e **le eventuali ulteriori** misure di sicurezza da adottare, formalizzate in un piano operativo per la loro messa in funzione. In particolare, le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

– **prevenzione**: attività che permette di ridurre/impedire gli incidenti di sicurezza, agendo direttamente sulla diminuzione delle probabilità di manifestazione reale di tali incidenti;
– **protezione:** attività che permette di ridurre/eliminare la gravità degli effetti nocivi dell'accadimento negativo.

Dopo aver individuato e valutato i fattori di rischio connessi alle risorse e ai beni da proteggere, vengono identificate le misure di prevenzione e protezione più idonee ad eliminare o ridurre il rischio al livello ritenuto accettabile.

Le misure intraprese o in programma sono sia tecniche che organizzative che di verifica.

In particolare, ai sensi delle normative vigenti in materia di privacy, l'ARNAS ha individuato alcune regole generali al fine di garantire una corretta e prudente gestione dei dati e un adeguato controllo dei possibili eventi dannosi, e precisamente:

– gli archivi o gli armadi contenenti dati sensibili o giudiziari sono chiusi a chiave;
– i dati sono custoditi con cura negli armadi e nei contenitori;
– la qualità dei locali, nonché degli armadi e dei contenitori ove sono conservati i dati, è ragionevolmente adeguata a preservare l'integrità degli stessi dai rischi legati a eventi distruttivi, accidentali, dolosi o dovuti a incuria ( presso il P.O. Garibaldi di Nesima i locali sono dotati di impianti di allarme antincendio e per il P.O. Garibaldi Centro è già stato predisposto il progetto di adeguamento antincendio);
– i documenti che contengono dati non rimangono mai incustoditi su scrivanie o tavoli di lavoro;
– i dati personali non sono condivisi, comunicati o inviati a terzi, se non previa autorizzazione;

– i documenti inviati via fax dopo la trasmissione vengono archiviati allegando il rapporto di trasmissione stampato dall'apparecchio;
– l'accesso ai locali dopo l'orario di chiusura è consentito al personale addetto alle pulizie o ad altri interventi sull'edificio (operai, elettricisti, ecc.), munito di cartellino di identificazione.
- al fine di rendere edotto il personale sui possibili rischi relativi al trattamento e sulle minacce alla sicurezza delle informazioni,l'ARNAS Garibaldi" ha intrapreso, nel contesto delle strategie organizzative, finalizzate all'osservanza della privacy, la progettazione di interventi formativi, rivolti sia al profilo sanitario che amministrativo.
Tali percorsi formativi, i cui destinatari sono sia i Responsabili che gli incaricati nel trattamento dei dati, sono accreditati dal Ministero della Salute, nell'ambito dei programmi di Educazione continua medica realizzati dall'ARNAS.
Nel corso del 2013 e del 2014 sono stati effettuati n. 8 corsi sui contenuti e sul significato del DL 196/2003 ai Responsabili del trattamento dati di ciascuna U.O. Questi ultimi hanno il compito di sensibilizzare direttamente i loro colleghi sui temi trattati.
La formazione interessa sia gli aspetti giuridici in materia di privacy, sia quelli peculiari dei trattamenti effettuati.

## 6. Trattamento con l'ausilio di strumenti elettronici (elaboratori in rete privata)

L'Azienda dispone di una rete privata (o rete LAN) cui sono allacciati tutti gli elementi hardware/elettronici nell'ambito della stessa struttura, sulla quale possono viaggiare i dati elettronici di proprietà.
Tutte le unita organizzative, sono collegate direttamente, alla sede legale dell'Azienda, conseguentemente, tutti i dati elettronici trattati presso le unità organizzative alla fine del ciclo di trattamento, risiedono fisicamente in apposite banche-dati elettroniche (specifiche per i vari sistemi informatici impiegati).
Tutti gli utenti perciò, attraverso i vari PC collegati e distribuiti nell'ambito dell'intera struttura (postazioni fisse-client) e dopo il superamento di apposite procedure di autenticazione ed autorizzazione possono accedere ai dati contenuti in una delle suddette banche dati, utilizzando lo specifico sistema informatico di riferimento.
Tutti gli utenti autorizzati, attraverso i vari PC collegati e distribuiti nell'ambito dell'intera Azienda

(postazioni fisse-client), possono collegarsi alla rete pubblica per l'accesso, attraverso appositi sistemi informatici, ad alcune banche dati elettroniche messe a disposizione dalla Regione.
Ove autorizzati inoltre, gli utenti possono accedere anche ad Internet, attraverso i vari PC collegati e distribuiti nell'ambito dell'intera Azienda.
Al fine di aumentare i livelli di sicurezza, per l'accesso ai dati e per l'uso delle risorse informatiche, in atto i Sistemi Informatici hanno predisposto quanto necessario per l'avvio e l'implementazione dell'Active Directory.
L'Active Directory è un insieme di servizi di rete meglio noti come directory service adottati dai sistemi operativi microsoft a partire da Windows 2000 Server.
L'insieme dei servizi di rete di Active Directory, ed in particolare il servizio di autenticazione Kerberos, realizzano un'altra delle caratteristiche importanti: il Single Sign-On (SSO). Tramite tale meccanismo un utente, una volta entrato nel dominio ed effettuato quindi il login ad esso da una qualsiasi delle macchine di dominio, può accedere a risorse disponibili in rete (condivisioni, mailbox, intranet ecc.) senza dover rieffettuare l'autenticazione. Questo facilita di molto gli utenti differentemente da quanto accade nelle reti peer to peer.

### 6.1 Locali CED

Il sistema di lavoro della struttura avviene con elaborazione in rete privata/pubblica.
Si dispone di una rete, realizzata mediante collegamenti via cavo e VPN costituita da:

- n.9 Server "Virtuali" e n. 3 Server " Fisici", localizzati presso il Centro Gestione Sistemi Informativi del P.O. Garibaldi Centro;
- n. 3 Server "Virtuali" e n. 2 Server " Fisici", localizzati presso il Centro Gestione Sistemi Informativi del P.O. Garibaldi di Nesima;
- n. 1 dispositivo di backup (NAS) localizzato presso il Centro Gestione Sistemi Informativi del P.O. Garibaldi Centro, dimensionato e adeguato alle esigenze operative;
- n. 1 dispositivo di backup (NAS) localizzato presso il Centro Gestione Sistemi Informativi del P.O. Garibaldi di Nesima, dimensionato e adeguato alle esigenze operative;
- Server per la gestione delle apparecchiature elettromedicali gestiti dalle Ditte erogatrici di servizi:

  G. E. Medical Sistems

Carestream
MEDIPASS
VARIAN

- Server NOEMA LIFE ( Laboratori Analisi dei due Presidi)

## 6.2 Sicurezza materiale e ambientale

Al fine di prevenire gli accessi non autorizzati, la sottrazione, il danneggiamento o la compromissione dei beni, l'interruzione delle attività o il furto di informazioni, l'ARNAS ha posto in essere le seguenti misure e controlla l'applicazione delle stesse:

- chiusura dei varchi non accessibili al pubblico, gestione continuativa dell'accesso controllato nei locali ed uso di cartelli indicatori/limitatori;
- protezione dei luoghi adibiti ad archivio;
- acquisizione e manutenzione di sistemi idonei alla conservazione di documenti e supporti contenenti dati sensibili o di particolare criticità per l'ARNAS;
- chiusura delle porte di accesso ai locali al di fuori dell'orario di servizio;
- manutenzione ordinaria, periodica e costante dei mezzi antincendio;
- revisione e manutenzione periodica delle serrature degli armadi e delle porte.

## 6.3 Gestione dei sistemi e delle reti

Lo scopo è quello di garantire, attraverso apposite procedure relative alle misure di sicurezza, il corretto e sicuro trattamento delle informazioni, la loro integrità e disponibilità, minimizzare il rischio di danni ai sistemi, assicurare la salvaguardia delle informazioni nelle reti e la protezione delle infrastrutture di supporto, prevenire i danni ai beni, l'interruzione delle attività, sottrazioni, modificazioni o uso improprio di informazioni scambiate con altre organizzazioni.

Al fine di assicurare il corretto e sicuro funzionamento dei sistemi di elaborazione e delle reti l'Azienda provvede con continuità:

- a proteggere l'integrità del software e delle informazioni con opportuni dispositivi antiintrusione (firewall, ecc...) ;
- a garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di rete provvedendo ad isolare le centraline telematiche a cui potrà accedere solo il personale designato;

- a evitare la perdita, modifica o uso improprio delle informazioni scambiate in rete formando gli operatori sul corretto utilizzo delle tecnologie Internet ed Intranet;
- a verificare che gli accessi, alla rete interna ed esterna e alla posta elettronica, siano effettuati solo da personale autorizzato;
- a verificare che la rete sia utilizzata solo per scopi istituzionali dell'ARNAS.

### 6.4 Software non autorizzati

E' vietata l'installazione di software copiato o, in ogni caso, privo di licenza d'uso.
Ogni utente è responsabile dell'utilizzo del software.

### 6.5 Software antivirus

Tutti i PC sono dotati di software antivirus.
Tali software vengono regolarmente aggiornati.

### 6.6 Controllo degli accessi

Gli obiettivi sono di controllare l'accesso alle informazioni, prevenire l'accesso non autorizzato alle informazioni, rilevare attività non autorizzate.
Al fine di raggiungere tali obiettivi l'ARNAS provvede a mettere in atto o a monitorare l'esecuzione dei seguenti processi.

### 6.7 Autorizzazione

Per autorizzazione si intende 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 dell'incaricato, ossia dell'insieme d'informazioni, univocamente associate allo stesso, che consente di identificare a quali dati esso può accedere, nonché i trattamenti ad esso consentiti.
I profili di autorizzazione, per ciascun incaricato o classi omogenee di incaricati, saranno individuati e configurati in modo da **limitare l'accesso ai soli dati** necessari per effettuare le **operazioni di trattamento**. Periodicamente, e comunque almeno *annualmente*, verrà verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

I dispositivi ed i software per il trattamento dei dati saranno aggiornati per il conseguimento di tali risultati.

### 6.9 Credenziali elettroniche: disattivazione a tempo

Per le topologie di reti locali (LAN) in architettura client/server, in cui il server accentra le risorse per il trattamento dei dati, verrà implementato o mantenuto sotto controllo un sistema di autorizzazione allo scopo di controllare la temporalità di utilizzo delle credenziali di autenticazione (password). Il sistema di autorizzazione è configurato al fine di raggiungere i seguenti obiettivi:

- riconoscere l'utente che si collega alla rete;
- consentire all'utente il cambio password al primo utilizzo;
- consentire all'utente di sostituire la password con cadenza almeno semestrale per coloro che trattano dati comuni;
- consentire l'utente a sostituire la password con cadenza almeno trimestrale per coloro che trattano dati sensibili e critici;
- disattivazione a tempo delle password non utilizzate per più di sei mesi consecutivi, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

### 6.10 Misure logiche di accesso ai dati

Ogni incaricato è dotato di credenziali di autenticazione; l'autenticazione consente l'accesso ad uno specifico trattamento o ad un insieme di trattamenti.

Al codice di autenticazione dell'incaricato è associata una parola chiave riservata (password), conosciuta solo dall'incaricato.

Gli incaricati sono informati sulle modalità di custodia dei codici ricevuti al fine di preservarne la segretezza.

Le parole chiave devono rispettare gli *standards* minimali richiesti sufficienti a renderne massima la sicurezza d'uso: minimo 8 caratteri, stringa costruita senza riferimenti all'incaricato, modifica ogni 6 mesi (ogni 3 mesi nel caso di trattamento di dati sensibili).

Il codice di identificazione è rigorosamente assegnato all'incaricato e non può essere successivamente assegnato ad altri soggetti e dopo 6 mesi di inutilizzo deve essere disattivato.

E' fatto obbligo agli incaricati al trattamento dei dati di :

- custodire con assoluta riservatezza e di non divulgare a terzi i dispositivi di accesso credenziali di autenticazione e parola chiave riservata (USERNAME e PASSWORD);
- non lasciare incustodito ed accessibile l'elaboratore elettronico durante una sessione di trattamento.

## 6.11 Interventi di Manutenzione

Quando, su un elaboratore, è richiesto un intervento di manutenzione, ordinaria o straordinaria, in loco o in laboratorio, sarà cura del responsabile concordare modi e tempi di intervento con i tecnici addetti.

Se l'intervento necessita dell'accesso all'elaboratore con le credenziali dell'incaricato, queste saranno inserite dallo stesso e non comunicate ai tecnici.

Nel caso che il dipendente non possa presenziare all'intervento, questi comunicherà le proprie credenziali al tecnico e provvederà a modificarle una volta terminato l'intervento.

Le società che effettuano manutenzione dei sistemi hardware o software sono considerate responsabili dei dati e devono, a tale scopo, rispettare le seguenti cautele:

- non effettuare copie né procedere alla eliminazione degli archivi informatici di titolarità dell'ARNAS;
- informare preventivamente gli interessati del giorno e dell'orario in cui saranno effettuati gli interventi tecnici;
- eventuali interventi remoti di assistenza mediante collegamento devono essere preventivamente autorizzati ;
- sottoscrivere impegno formale al rispetto di tutte le norme e del presente documento.
- usare riservatezza su dati ed informazioni addivenuti in loro possesso.

## 6.12 Gestione della continuità del servizio (backup e ripristino)

Gli obiettivi sono di contrastare efficacemente le eventuali interruzioni delle attività e dei processi di servizio critici, causati da malfunzionamenti, da eventuali avvenimenti straordinari o da gravi danni o disastri.

In tale ottica le procedure di salvataggio e ripristino dei dati costituiscono un punto nodale nelle politiche di sicurezza dell'ARNAS.

La perdita dei dati, evento che può accadere per cause diverse quali errori materiali, azione di virus, malfunzionamento degli strumenti, eventi naturali o dolosi, rappresenterebbe per l'ARNAS un avvenimento disastroso.

A fronte delle precedenti considerazioni l'adozione di un efficiente ed efficace sistema di back up, ossia produrre copie di riserva dei dati, diventa un'attività fondamentale nella realtà aziendale.

Le misure che l'ARNAS adotta, ed intende adottare laddove non presenti, per contrastare tali evenienze sono le seguenti:

- Acquisizione ed installazione di dispositivi di back up (masterizzatore, ecc...) sui computer sprovvisti di tali dispositivi soprattutto se trattasi di PC stand alone.
- Tutti gli utenti, opportunamente istruiti, sono responsabili delle operazioni di salvataggio dei dati memorizzati sui propri computer;
- Il Backup dei dati deve essere effettuato con frequenza *almeno settimanale*;
- I supporti che contengono il salvataggio dei dati devono essere conservati in appositi armadi ed in luoghi decentrati rispetto al locale in cui si trovano i server;
- I supporti di memorizzazione, che contengono il salvataggio di dati sensibili, non più idonei all'uso, devono essere distrutti meccanicamente;
- Si devono utilizzare idonee procedure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni. Per verificare la correttezza delle procedure di ripristino devono essere previste prove di funzionamento almeno con cadenza trimestrale o ogni volta che variano le procedure stesse. Eventuali malfunzionamenti devono essere verbalizzati in modo da tenerne traccia per successive prove e miglioramenti. Ogni incaricato al trattamento dei dati è responsabile della corretta esecuzione delle operazioni di back up e di ripristino.

## 7. Monitoraggio settoriale dell'attuazione delle misure di sicurezza

La verifica dell'efficacia e della validità nel tempo delle misure di sicurezza adottate è un punto fondamentale di tutto il processo per la sicurezza.
L'efficacia di una soluzione adottata si può valutare solo "monitorando" nel tempo gli effetti di questa soluzione. La bontà delle misure adottate deve essere periodicamente verificata.
Ogni responsabile è tenuto a monitorare l'applicazione delle misure di sicurezza e a valutarne l'efficacia.
Il controllo dell'efficacia delle misure adottate dovrà essere focalizzato almeno sui seguenti aspetti:

- Efficienza e utilizzo delle misure di sicurezza;

- Accesso fisico ai locali ove si svolge il trattamento;
- Procedure di archiviazione e custodia dei dati trattati;
- Integrità dei dati e delle copie di backup;
- Distruzione e/o formattazione dei supporti magnetici non più utilizzati;

- Corretto utilizzo delle parole chiave (password) e dei profili di accesso degli incaricati;
- Disattivazione dei codici di accesso non utilizzati per più di sei mesi;
- Verifica del livello di formazione degli incaricati, prevedendo sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica.

## 8. Protezione degli ambienti fisici: misure adottate

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.

a) Controllo di accesso ai locali

I locali adibiti a CED (locale server) sono allocati presso il P.O. Garibaldi Centro e Presso il P.O. Garibaldi Nesima, che sono sorvegliati sorvegliata in orario lavorativo, e soggetti ad accesso limitato. La porta di accesso ai locali è mantenuta costantemente chiusa a chiave.

I locali sono dotati di gruppi di continuità, condizionatori ed estintori.

b) Autorizzazioni all'ingresso nei locali

Hanno accesso ai locali server: gli addetti e gli addetti del servizio di assistenza informatica.

## 9. Trattamento senza l'ausilio di strumenti elettronici

Ai sensi dell'art.35 del D.Lgs. 196/2003:

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità operative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

### 9.1 Documenti cartacei

I supporti cartacei contenenti i dati personali, vengono archiviati, una volta terminato il ciclo lavorativo, in locali, schedari, armadi, cassetti dotati di chiave.

Gli archivi cartacei si distinguono in:

- archivi correnti (insieme dei documenti correnti): tenuti dai singoli Incaricati e/o Responsabili negli uffici e nelle aree operative o tenuti dal personale nei reparti di cura;
- archivi di deposito (insieme dei documenti semi-attivi): archivi ad accesso ristretto presenti in alcune unità operative mantenuti a cura del relativo Responsabile o Incaricato;
- per quanto attiene gli archivi centralizzati l'ARNAS ha affidato il Servizio di Archiviazione e Gestione della documentazione sanitaria ed amministrativa all'ATI composta dalle Ditte "Gestione Archivi "s.r.l. e "Sikelia Service" i cui rappresentanti legali sono stati nominati Responsabili esterni del trattamento.

Copia della lettera di nomina, controfirmata dagli interessati, viene conservata a cura della Segreteria della Commissione per il Diritto alla Riservatezza dei dati.

La Documentazione Sanitaria tenuta dall'Azienda è stata limitata agli ultimi due anni.

- archivi storici (insieme dei documenti storici): archivi mantenuti per motivi storici o per esigenze di legge: questi archivi a breve saranno consegnati alla Ditta di cui sopra.

E' stata emanata, diffusa e pubblicata sull'INTRANET Aziendale, nell'applicativo "Direzione Sanitaria – Qualità & Accreditamento" la "PROCEDURA DI CORRETTA COMPILAZIONE E GESTIONE DELLA CARTELLA CLINICA"

## 10. Misure fisiche di accesso ai dati

Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono

controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate.

## 11. Misure connesse alla "Sorveglianza sanitaria e sicurezza nei luoghi di lavoro" (ai sensi del Decreto legislativo n. 81 del 9 aprile 2008 e successive modificazioni).

L'attività relativa alla sorveglianza sanitaria e sicurezza nei luoghi di lavoro è realizzata, nell'Ente, in modo accentrato tramite il Servizio di Prevenzione e Protezione e l'Ufficio del Medico Competente che collaborano con i datori di lavoro delegati e gli RLS.
In adesione a quanto previsto dall'articolo 53 del Decreto legislativo n. 81/2008 "Tenuta documentazione", l'ARNAS consente l'accesso ai dati solo ai datori di lavoro, a richiesta agli RLS e ai soggetti espressamente abilitati dal datore di lavoro.
I documenti sono conservati sia su supporto cartaceo che informatico.
Il documento relativo al giudizio di "idoneità totale" alla mansione, di "idoneità parziale" (temporanea o permanente) con o senza prescrizioni e/o limitazioni, di "inidoneità" (temporanea o permanente) viene protocollato e inviato in busta chiusa al Datore di Lavoro e al lavoratore " brevi manu" .
I dati biostatici sono archiviati sul computer su un apposito programma a cui può accedere solo il personale afferente all'U.O.

## 12. Pianificazione degli interventi formativi previsti

Per il 2015 sono stati organizzati n. 8 eventi formativi per il personale sanitario e per il personale amministrativo.
In particolare, per quanto attiene alle azioni *informative*, il presente documento, verrà inviato ai Responsabili delle UU.OO e Servizi affinché ne diano la massima diffusione ad ogni livello aziendale e venga pubblicato sul sito Internet dell'ARNAS e sull' INTRANET aziendale.
Inoltre agli incaricati sono state impartite apposite istruzioni generali su come devono essere trattati i dati personali e le procedure da seguire per la raccolta, elaborazione ed archiviazione dei dati e dei documenti, nonché le modalità di custodia degli stessi.
La formazione dovrà essere programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi strumenti, rilevanti rispetto al trattamento dei dati personali.

## 13. Videosorveglianza

L'Azienda si sta attivando per l'attività di video sorveglianza mediante videocamere a circuito chiuso all'interno delle pertinenze aziendali, per motivi di sicurezza e vigilanza su eventuali attività illecite ai danni di beni o persone, controllo accessi. Chi accede in una zona videosorvegliata ne viene informato a mezzo di idonea informativa, che offre gli elementi previsti dall'Autorità Garante nel modello semplificato di informativa "minima" da essa proposto. Il supporto con l'informativa sarà collocato nei luoghi ripresi o nelle immediate vicinanze.

In luoghi diversi dalle aree esterne il modello sarà integrato con un avviso circostanziato che riporti gli elementi del dell'art. 13 del Codice.

## 14. Conformità

Al fine di garantire il rispetto delle norme civili, penali, regolamentari o contrattuali l'ARNAS vigilerà affinché ci sia piena conformità alle stesse.
L'ARNAS assicura la conformità degli standard alle politiche di sicurezza e l'effettuazione di audit per massimizzare l'efficacia del sistema di sicurezza e minimizzare le intromissioni.