REGIONE SICILIANA

Azienda Ospedaliera di Rilevanza Nazionale e di Alta Specializzazione

"GARIBALDI"

Catania

VERBALE DI DELIBERAZIONE DEL COMMISSARIO STRAORDINARIO n. 145

Oggetto: **Approvazione del Regolamento Aziendale sulla Protezione dei Dati.**

SISTEMA INFORMATICO AZIENDALE

Bilancio
Aggregato di spesa:
Sub aggregato di spesa:
Autorizzazione n. _____ - Sub _____
Conto Ec.

Si attesta che la disponibilità del fondo del sopra riportato sub-aggregato è sufficiente a coprire la spesa prevista dal presente atto.

Per l'Ufficio Riscontro _____

Il Responsabile del Settore _____

SETTORE ECONOMICO FINANZIARIO PATRIMONIALE
Visto:
Si conferma la suindicata disponibilità rilevata dal Servizio Informatico Aziendale e si iscrive nelle pertinenti utilizzazioni del budget.

Catania _____

L'addetto alla verifica della compatibilità economica

_____

Lista di liquidazione n.

_____

_____

Il Dirigente Responsabile del Settore Economico Finanziario
(Dott. Gianluca Roccella)

_____

Settore:

Il Dirigente Responsabile del Servizio Informatico Aziendale
Ing. Mario BISIGNANO

_____

Il Responsabile della Protezione dei Dati
Dott. Davide Morales

Seduta del giorno 30 OTT. 2018

Nei locali della sede legale dell'Azienda piazza S. Maria di Gesù, 5 Catania

IL COMMISSARIO STRAORDINARIO
dott. Giorgio Giulio SANTONOCITO

Nominato con Decreto Assessoriale n. 1664 del 20.09.2018, ai sensi dell'art. 20, c. 3 della L.R. 5/2009 e sm.i. e dell'art. 2, c. 2 del D.Lgs 171/2016 e s.m.i

Con la presenza del:

Direttore Amministrativo
Dott. Giovanni ANNINO

_____

Con l'assistenza, quale Segretario del Dott. **DOTT. FRANCESCO GIOVANNI MARANGIA**

_____

ha adottato la seguente deliberazione

PREMESSO

- che il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (regolamento generale sulla protezione dei dati)
- che a decorrere dal 25.05.2018, è diventato operativo il Nuovo Regolamento Europeo sulla Protezione dei dati personali UE 206/679;
- che è stato emanato il Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU n.205 del 4-9-2018) - Vigente al: 19-9-2018;
- che con nota prot. N. 40084 del 23.05.2018 e acquisita con prot. N° 0009133 del 23/05/2018, l'Assessorato della Salute della Regione Sicilia – Ufficio di diretta collaborazione dell'Assessore ha definito le prescrizioni da osservare ed applicare in merito al GDPR;
- che il Responsabile della Protezione dei Dati, nominato con Deliberazione n. 556 del 23.05.2018 ha trasmesso con nota prot. n° 11/RPD-SIA-DA al Responsabile SIA il Regolamento Aziendale sulla Protezione dei Dati;

RITENUTO che il suddetto "Regolamento Aziendale sulla Protezione dei Dati" è in linea con la normativa di riferimento di cui al Regolamento Generale sulla Protezione dei Dati (UE) 2016/679;

VISTO il Regolamento Aziendale sulla Protezione dei Dati (qui allegato *sub littera A*) predisposto dal Responsabile della Protezione dei Dati Dott. Davide Morales;

Su proposta del Responsabile del Servizio Informatica Aziendale che con la sottoscrizione del presente atto ne attesta la correttezza sia formale che sostanziale;

Sentito il parere del Direttore Amministrativo,

D E L I B E R A

per i motivi esposti in premessa, che qui si intendono ripetuti e trascritti di:

- approvare l'allegato "Regolamento Azienda sulla Protezione dei Dati" della presente deliberazione, in linea con la normativa di riferimento di cui al Nuovo Regolamento Europeo sulla Protezione dei Dati (UE) 2016/679", al Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU n.205 del 4-9-2018) - Vigente al: 19-9-2018;
- dare mandato al Servizio Informatica Aziendale di pubblicare il nuovo "Regolamento

Aziendale sulla protezione dei Dati", sul sito istituzionale dell'Azienda (Intranet e Internet);

- dare immediata esecutività al presente provvedimento stante la necessità di procedere celermente all'adeguamento alle novità in materia.

ALLEGATI:

"A" – Regolamento sulla Protezione dei Dati ";

Il Responsabile UO Servizio Informatico Aziendale
Ing. Mario BISIGNANO

IL DIRETTORE AMMINISTRATIVO
(Dott. Giovanni ANNINO)

IL COMMISSARIO STRAORDINARIO
(Dott. Giorgio Giulio SANTONOCITO)

Il Segretario
DOTT. FRANCESCO GIOVANNI MARANGIA

Copia della presente deliberazione è stata pubblicata all'Albo dell'Azienda il giorno ..... e ritirata il giorno .....

L'addetto alla pubblicazione

.....

Si attesta che la presente deliberazione è stata pubblicata all'Albo della Azienda dal ..... al ..... - ai sensi dell'art.65 L.R. n.25/93, così come sostituito dall'art.53 L.R. n.30/93 - e contro la stessa non è stata prodotta opposizione.

Catania.....

Il Direttore Amministrativo

.....

Inviata all'Assessorato Regionale della Salute il ..... Prot. n. .....

Notificata al Collegio Sindacale il ..... Prot. n. .....

La presente deliberazione è esecutiva:

- [x] immediatamente
- [ ] perché sono decorsi 10 giorni dalla data di pubblicazione
- [ ] a seguito del controllo preventivo effettuato dall'Assessorato Regionale per la Sanità:
  a. nota di approvazione prot. n. ..... del.....
  b. per decorrenza del termine

IL FUNZIONARIO RESPONSABILE

_____

ARNAS GARIBALDI CATANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE

AZIENDA OSPEDALIERA

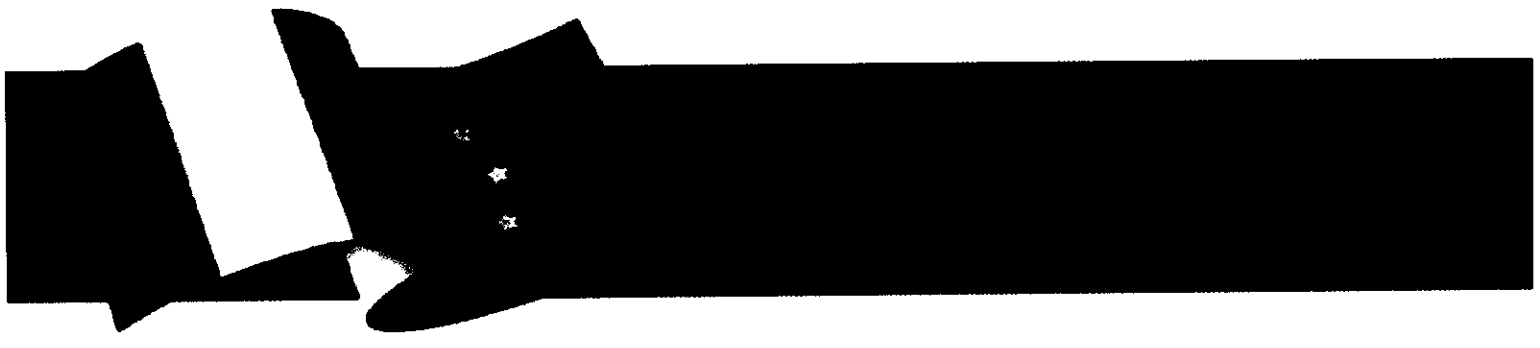
DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE "GARIBALDI"

Catania

REGOLAMENTO SULLA PROTEZIONE DEI DATI

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Responsabile della Protezione Dati: Dott. Davide Morales



INDICE

ART. 1 – Principi e Finalità

Il 4 maggio 2016 è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE* (regolamento generale sulla protezione dei dati) . Inoltre, preso atto del Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU n.205 del 4-9-2018) - Vigente al: 19-9-2018

Al fine di garantire all'interno dell'Azienda Garibaldi puntuale applicazione del Regolamento generale sulla protezione dei dati UE 2016/67 (di seguito denominato "Regolamento"), la Direzione Generale emana il seguente Regolamento interno, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza ed alla identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda.

ART. 2 - Definizioni

Nel trattamento dei dati personali l'Azienda adotta le definizioni di cui all'Art. 4 del Regolamento, con particolare riferimento a:

«**trattamento**»: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati;

«**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze professionali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

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

«**dati identificativi**»: i dati personali che permettono l'identificazione diretta dell'interessato;

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

«**dati giudiziari**»: i dati personali idonei a rivelare i provvedimenti di cui all'art. 3, comma 1, lettere da a) ad o) e da r) a u) del D.P.R.

14.11.2002, n.313, in materia di casellario giudiziario, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o indagato, ai sensi degli articoli 60 e 61 del Codice di Procedura Penale;

«**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«**titolare**»: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine all'assunzione delle decisioni sulle finalità, modalità e strumenti utilizzati per il trattamento dei dati personali, ivi compreso il profilo della sicurezza;

«**responsabile**»: la persona fisica, la persona giuridica, la pubblica amministrazione, e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali;

«**addetti al trattamento**»: le persone fisiche, autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

«**interessato**»: la persona fisica, la persona giuridica, l'ente Il' associazione cui si riferiscono i dati personali;

«**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;

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

«**dato anonimo**»: il dato che in origine, o seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

«**blocco**»: conservazione di dati personali, con sospensione temporanea di ogni operazione di trattamento;

«**banca dati**»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

«**amministratore di sistema**»: il Responsabile Servizi Informativi, nominato dal titolare, destinato a sovrintendere alle risorse dei sistemi operativi degli elaboratori, delle banche dati e del sistema informativo in generale.

Per tutte le altre definizioni, non contenute nel presente articolo, si fa espresso richiamo all'art. 4 del Nuovo Regolamento Europeo.

ART. 3 – Titolare del Trattamento

Il titolare del trattamento dei dati personali ai sensi e per effetti del Codice è l'Azienda Ospedaliera "Garibaldi", nel suo complesso, rappresentato dal Direttore Generale, in qualità di rappresentante legale dell'Azienda stessa.

Il titolare, avvalendosi della collaborazione del Responsabile della Protezione dei Dati provvede:

1. tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario;
2. al rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento;
3. ad un meccanismo di certificazione che può essere utilizzato come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

ART. 4 – Trattamento dei dati personali

Qualunque trattamento dei dati personali posto in essere dall' Azienda è consentito, fatto salvo il rispetto dei presupposti e dei limiti stabiliti dal Regolamento, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti, soltanto per lo svolgimento delle funzioni istituzionali di propria competenza.

Pertanto, oggetto del trattamento devono essere solamente i dati personali per lo svolgimento di attività istituzionali.

I dati personali devono essere trattati soltanto per il tempo necessario all'espletamento del servizio, in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e devono anche essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per le 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 stato consentito, anche quando i dati sono raccolti nello svolgimento di attività di vigilanza, ispettive o di controllo.

Il trattamento dei dati sensibili è invece consentito solo se autorizzato da espressa disposizione di legge nella quale siano espressamente specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui una disposizione specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in relazione ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare di cui al Regolamento Europeo 2016/679.

ART.5 – Responsabili del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche

organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. Il Responsabile esterno o interno è nominato dal titolare con atto formale.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. Al Responsabile spetta in generale il compito di garantire il pieno rispetto delle leggi in materia ed in particolare:
    - individuare, formare e nominare gli incaricati del trattamento e successivamente diramare le istruzioni scritte necessarie per un corretto, lecito, sicuro trattamento;
    - attuare gli obblighi di informazione e acquisizione del consenso, quando richiesto, nei confronti degli interessati;
    - vigilanza circa la corretta custodia e conservazione delle password e delle chiavi d'accesso agli armadi per la conservazione dei supporti magnetici o cartacei;
    - controllo sulla effettiva adozione, da parte degli incaricati, di tutte le misure necessarie perché il trattamento dei dati personali avvenga nel pieno rispetto delle disposizioni di legge in materia e di quelle del Regolamento interno dell'ARNAS Garibaldi;
    - vigilanza sul rispetto dei diritti di accesso degli interessati e con le modalità previste dalle norme di legge sopra richiamate;
    - rispetto della sicurezza nel trattamento dei dati quanto alla custodia, alla cessazione e ai limiti di utilizzabilità, secondo quanto previsto dal Regolamento interno o dove non indicato dalla normativa vigente;
    - garantire all'interessato l'effettivo esercizio dei diritti previsti dal Regolamento (UE) 2016/679, in ordine, ove possibile, all'accesso ai dati e a tutti i diritti di aggiornamento, rettificazione, cancellazione e di opposizione;
    - collaborare per l'attuazione delle prescrizioni del Garante;
    - predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni del Regolamento Aziendale sulla protezione dei dati, nonché adeguare il sistema alle norme regolamentari in materia di sicurezza, curandone l'applicazione da parte degli incaricati.
    - Comunicare tempestivamente qualunque richiesta di accesso, accesso non autorizzato o eventuale anomalia di sicurezza del sistema al Responsabile della Protezione dei Dati Personali.

ART. 6 – Persone autorizzate al trattamento

Il Responsabile del trattamento designa le persone fisiche autorizzate al trattamento dei dati a svolgere le operazioni di sua competenza precisando, con le istruzioni ricevute dal Titolare, i relativi compiti, l'ambito del trattamento consentito e le modalità cui devono attenersi.

Gli autorizzati sono individuati dal Responsabile, con apposito atto formale nel quale debbono essere espressamente precisati gli "ambiti" del trattamento consentito.

Gli autorizzati al trattamento devono osservare tutte le istruzioni scritte, loro impartite dal Responsabile.

Essi hanno accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti istituzionali loro assegnati. Durante il trattamento e, soprattutto, in caso di allontanamento dal posto di lavoro, l'autorizzato al trattamento dei dati deve osservare tutte le misure previste ed a sua disposizione, secondo le istruzioni ricevute dal Responsabile del trattamento, per evitare l'accesso non autorizzato di terzi, anche se dipendenti, ai dati personali trattati o in corso di trattamento. A prescindere, comunque, dalla formale attribuzione della qualifica di "Persona autorizzata al trattamento", i dipendenti dell'Azienda, nonché tutti coloro che vi operano, a qualsiasi titolo, con o senza retribuzione, anche in regime di convenzione con le Università, gli specializzandi, i tirocinanti ed i volontari, sono tenuti al rispetto di quanto previsto dal presente regolamento, qualora durante la loro attività vengano a conoscenza di dati personali.

Tutti i soggetti di cui sopra, in particolare, sono tenuti a:

- osservare tutte le istruzioni, più in generale impartite a livello aziendale, dal titolare, dai responsabili e dal Responsabile per la protezione dei Dati (RPD), in ordine al trattamento dei dati personali ed ai connessi profili della sicurezza;
- astenersi da qualunque comportamento o operazione, inerente al trattamento dei dati personali, che non sia coerente con l'espletamento dei propri compiti istituzionali;
- impegnarsi a non comunicare e diffondere all'esterno dell'Azienda, per finalità diverse da quelle del rapporto di lavoro, i dati personali di cui siano venuti comunque a conoscenza.

Le lettere di nomina dei Responsabili e gli elenchi delle persone autorizzate al trattamento sono conservati dal Titolare, il quale dispone di un quadro completo di chi fa cosa nell'ambito del trattamento dei dati personali.

Le lettere di incarico, firmate per ricevuta dagli addetti al trattamento, vengono conservate dai singoli Responsabili che le hanno emesse.

Periodicamente, con cadenza almeno annuale, si procede ad aggiornare la definizione dei dati cui gli addetti al trattamento sono autorizzati ad accedere e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione e/o della manutenzione degli strumenti elettronici.

ART 7 - Informativa

L'Interessato ha il diritto di essere informato in modo trasparente, leale e dinamico sui trattamenti effettuati sui suoi dati. Pertanto, affinché un trattamento possa definirsi trasparente, chiaro e corretto, è necessario che all'interno sia resa un'informativa esaustiva sull'esistenza del trattamento e delle sue finalità. Il trattamento dei dati personali esige la

previa informativa dell'interessato, di cui all'art. 13 del Regolamento. L'informativa è sempre dovuta a prescindere dall'obbligo di acquisizione del consenso.

Essa deve contenere gli elementi tassativamente indicati dall'art.13 del Regolamento Europeo 2016/679, e più specificatamente:

- dati di contatto del **RPD-DPO** (Responsabile della Protezione dei Dati – Data Protection Officer);
- 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 (in particolare se i dati personali sono trasferiti in Paesi terzi ed in caso affermativo attraverso quali strumenti) o che possono venirne a conoscenza in qualità di responsabili o di incaricati e l'ambito di diffusione dei dati medesimi;
- specificare il periodo di conservazione;
- i diritti di cui all'articolo successivo;
- il diritto di presentare un reclamo all'autorità di controllo
- gli estremi identificativi del Titolare e del Responsabile del trattamento;

L'informativa *(disciplinata nello specifico dagli artt. 13 e 14 del regolamento)* deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. Inoltre, deve avere forma concisa, trasparente, intelligibile; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee.

ART. 8 – Nomina del Responsabile della Protezione dei Dati (RPD o Data Protection Officer DPO)

L'art. 37, par. 1, lett. a), del RGPD prevede che i titolari e i responsabili del trattamento designino un RPD «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali».

Il Responsabile della Protezione dei Dati, è nominato con atto formale dell'Amministrazione. Secondo l'art. 39 del Nuovo Regolamento Europeo 2016/679 svolge le seguenti funzioni:

1. *Informazione e consulenza* – il DPO si occuperà di informare, aggiornare e fornire consulenza ai responsabili dell'organizzazione in tema di privacy (titolare o responsabile del trattamento dei dati), così come a tutti i dipendenti, per ciò che riguarda gli obblighi normativi sulla privacy.
2. *Sorveglianza* – il DPO dovrà vigilare sull'osservanza del regolamento e delle altre normative europee e nazionali sulla privacy. Si dovrà occupare anche di attribuire le responsabilità in materia di protezione dei dati, di promuovere la formazione e sensibilizzare il personale sul tema.
3. *Valutazione* – il DPO su richiesta potrà fornire un parere di valutazione d'impatto sulla protezione dei dati.

4. *Cooperazione* – il DPO è richiesta la piena collaborazione con le autorità di controllo.
5. *Punto di contatto* – il DPO è l'interfaccia tra l'organizzazione e le autorità di controllo.

Il RGPD prevede, all'art. 38, par. 2, che «il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica».
L'ARNAS Garibaldi nomina con atto verbale di deliberazione del Commissario n° 556 del 23 maggio 2018 il Responsabile della Protezione dei Dati personali.

ART. 9 – Diritti dell'Interessato

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Diritto di Accesso (Art. 15 - UE/2016/679)

1 - L'interessato può, senza alcuna formalità, chiedere all'incaricato del trattamento dei dati di:

- prendere visione dei dati che lo riguardano;
- avere comunicazione dei dati in forma intelligibile;
- conoscere le finalità istituzionali per cui sono conservati i propri dati.
- Il periodo di conservazione dei dati personali

2 - L'interessato deve esibire al momento della richiesta un documento di identità. La persona fisica o giuridica che agisce su incarico dell'interessato deve presentare, unitamente alla delega sottoscritta, fotocopia della carta d'identità del delegante. In caso di decesso la richiesta può essere effettuata da chiunque ne abbia interesse (successori, rappresentanza legale, ecc).

3 - La richiesta non può essere rinnovata, salvo motivi specifici, prima di un intervallo pari a 90 gg.

4 - L'incaricato comunica i dati in suo possesso oralmente salvo diversa ed esplicita richiesta.

Cancellazione o trasformazione anonima dei dati. (Art. 17 - UE/2016/679)

L'interessato può, senza formalità e senza spese, chiedere all'incaricato, ove i dati non siano più necessari per le finalità istituzionali dell'Azienda:

- la cancellazione dei dati posseduti;
- la trasformazione in forma anonima dei dati.

Aggiornamento, rettifica ed integrazione dei dati. (Art. 16 - UE/2016/679)

L'interessato può, senza formalità e senza spese, chiedere all'incaricato del trattamento dei dati:

- l'aggiornamento dei dati;
- la rettificazione dei dati;
- l'integrazione dei dati;

L'integrazione dei dati può avvenire solo qualora il richiedente dimostri di averne interesse e le motivazioni espresse rientrino tra le finalità istituzionali dell'Azienda.

Portabilità dei dati (Art. 20 - UE/2016/679)

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un titolare del trattamento e ha il diritto di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti da parte del titolare cui li ha forniti.

Opposizione al trattamento dei dati (Art. 21 - UE/2016/679)

. L'interessato può senza formalità e senza spese:

- opporsi al trattamento dei dati personali con finalità commerciale o di invio di informazione commerciale o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva;
- opporsi al trattamento dei propri dati personali ancorché pertinenti allo scopo della raccolta.

L'interessato che si oppone al trattamento dei propri dati deve indicare espressamente i motivi che legittimano la richiesta.

L'opposizione potrà essere accolta solo qualora non sia in contrasto con le disposizioni di legge o con le finalità istituzionali dell'Azienda.

ART. 10 – Obblighi dell'Interessato

L'Utente dell'Azienda è obbligato a fornire i dati personali o sensibili strettamente necessari ai fini istituzionali dell'Ente per potere accedere alle prestazioni richieste.

Sono fatti salvi i casi d'urgenza o di impossibilità temporanea a comunicare i dati.

ART. 11 – Consenso

Il **consenso,** in base al Regolamento Generale (art. 4 GDPR), è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
Il presupposto indefettibile è che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo.
L'età per esprimere il consenso al trattamento dei dati nell'ambito dei servizi viene fissata a 14 anni, utilizzando la deroga prevista dal Regolamento Europeo in tema di regolamentazione della tutela dei minori (che prevede un limite di 16 anni riducibile fino a 13).
Inoltre, in base al Considerando 32: "*il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.*
Il consenso deve essere, quindi:

- ✓ inequivocabile;
- ✓ libero;
- ✓ specifico;
- ✓ informato;
- ✓ verificabile;
- ✓ revocabile.

ART. 12 – Conservazione e sicurezza dei dati

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo tale da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distribuzione o di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito non conforme alle finalità di raccolta. L'accesso agli archivi aziendali deve essere controllato, e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura. Con riferimento agli archivi aziendali la responsabilità della conservazione e sicurezza dei medesimi spetta al responsabile competente per i dati oggetto del trattamento.

ART. 13 - Videosorveglianza

L'installazione di apparecchiature di videosorveglianza nell'Azienda è consentita dal Titolare, solo dopo attenta valutazione sulla proporzionalità fra lo strumento impiegato e gli scopi perseguiti (assistenza e cura dei pazienti ricoverati, sicurezza delle persone e delle attrezzature), e, in ogni caso, quando altre misure possibili siano concretamente insufficienti o inattuabili. Trova comunque applicazione, circa il divieto di controllo del lavoratore a distanza, l'intero dispositivo dell'art. 4, legge n.300/70 e s.m.i. . L'Azienda preso atto della necessità di regolamentare l'installazione dei sistemi di videosorveglianza, ha predisposto uno specifico regolamento approvato con verbale di deliberazione del Commissario n°606 del 4 giugno 2018 avente per oggetto "Approvazione del Regolamento Aziendale sulla videosorveglianza".

ART. 14 – Comunicazione e diffusione dei dati personali

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

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 e, in difetto, quando la stessa è, comunque, necessaria per lo svolgimento delle funzioni istituzionali dell'Azienda.

La comunicazione da parte di un soggetto pubblico a privati o ad 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.

Fermo restando quanto previsto dal presente regolamento, la comunicazione dei dati personali, inclusi quelli sensibili, trattati, per disposizione, di legge o di regolamento o, comunque, per il perseguimento di attività istituzionali, tra le diverse strutture organizzative aziendali, costituisce compito istituzionale e non richiede, pertanto, l'adozione di specifiche formalità, da parte delle strutture stesse.

È fatta salva, comunque, la comunicazione o la diffusione dei dati, che siano richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

ART. 15 – Comunicazione sullo stato di salute degli utenti

I dati personali idonei a rivelare lo stato di salute dell'interessato possono essere noti a quest'ultimo, per il tramite del medico dell'Azienda competente, in relazione ai provvedimenti organizzativi aziendali, ovvero per il tramite del medico di fiducia dell'interessato da lui designato, o del medico che ha prescritto il ricovero o gli accertamenti. Il Responsabile del trattamento dati può autorizzare, per iscritto, gli esercenti le professioni sanitarie, diversi dai medici, che, nell'espletamento dei propri compiti, intrattengono diretti rapporti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi risultati all'interessato; l'autorizzazione è, in tal caso, effettuata, in sede di designazione dei predetti esercenti, quali incaricati del trattamento dei dati, nel rispetto dei limiti imposti dalla normativa vigente. Nell' eventualità che l'interessato si trovi in stato di impossibilità fisica, incapacità di agire o di incapacità di intendere e di volere, le comunicazioni di cui ai commi precedenti, sono rese a chi dimostri, anche mediante autocertificazione, resa ex art.46, D.P.R. n.445/2000, di esercitare legalmente la potestà, ovvero di essere un prossimo congiunto, un familiare, un convivente, o, in loro assenza, il responsabile della struttura presso cui dimora. In occasione delle prestazioni di pronto soccorso o durante il ricovero, le informazioni di cui sopra possono essere note anche a soggetti diversi dall'interessato, dietro specifico consenso scritto di quest'ultimo.

ART. 16 – Rapporti tra diritto d'accesso e riservatezza

I presupposti, le modalità, i limiti per l'esercizio del diritto d'accesso a documenti amministrativi, contenenti dati

personali, e la relativa tutela giurisdizionale, restano disciplinati dalla L. 241/90 e s.m.i. e dalle altre disposizioni di legge in materia, nonché dal regolamento aziendale che disciplina il diritto di accesso, anche per ciò che concerne i dati sensibili e giudiziari e le operazioni di trattamento, eseguibili in adempimento di una richiesta di accesso.

Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Quando il trattamento concerne dati idonei a rilevare lo stato di salute o la vita sessuale, il trattamento è consentito, se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

ART. 17 – Cartelle cliniche

La cartella clinica costituisce, ad ogni effetto di legge un atto pubblico.

Essa deve essere redatta in forma intelligibile e coerentemente ai requisiti di veridicità e completezza.

Ogni annotazione va in essa trascritta, contemporaneamente all'evento descritto.

Nella cartella clinica, i dati relativi al paziente debbono chiaramente distinguersi da quelli eventualmente riguardanti altri interessati, ivi comprese le informazioni relative ai nascituri. In ordine alla conservazione del documento una circolare del Ministero della Sanità (n°900 2/AG454/260), emanata il 19 dicembre del 1986 stabilisce che "le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente, poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto. In merito alla conservazione delle radiografie, non rivestendo carattere di atti ufficiali, si ritiene che potrà essere sufficiente un periodo di 20 anni. La documentazione clinica deve essere custodita dal medico solo durante la fase di degenza del paziente, mentre al momento del passaggio della cartella clinica all'archivio centrale, la responsabilità si trasferisce al direttore sanitario dell'Ente/Presidio Ospedaliero. Per le cartelle cliniche in formato elettronico è responsabilità del Dirigente dei Sistemi Informatici dell'Ente attivare le procedure necessarie per garantire la sicurezza informatica e l'archiviazione dei dati.

Il rilascio delle copie di cartella clinica è consentita agli aventi diritto individuabili:

- nel paziente stesso
- nella persona fornita di delega conformemente alle disposizioni di legge
- negli enti previdenziali (INAIL-INPS)
- nell'Autorità Giudiziaria

Inoltre, all'interzo dell'Azienda Ospedaliera e durante il trasferimento del paziente da un Reparto di degenza ad un altro, la cartella clinica deve essere trasportata in busta chiusa e sigillata al fine di garantirne l'integrità e la lettura da personale non autorizzato.

Continuano, comunque, ad applicarsi tutte le restanti disposizioni di legge, in ordine alla loro compilazione e conservazione.

Eventuali richieste di presa visione o di rilascio di copia di 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:

- di far valere o di 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;
- 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 ed inviolabile.

ART. 18 – Trattamento di Dati Genetici

Si intende per:

a) dato genetico, il risultato di test genetici o ogni altra informazione che, indipendentemente dalla tipologia, identifica le caratteristiche genotipiche di un individuo trasmissibili nell'ambito di un gruppo di persone legate da vincoli di parentela;
b) campione biologico, ogni campione di materiale biologico da cui possono essere estratti dati genetici caratteristici di un individuo;
c) test genetico, l'analisi a scopo clinico di uno specifico gene o del suo prodotto o funzione o di altre parti del Dna o di un cromosoma, volta a effettuare una diagnosi o a confermare un sospetto clinico in un individuo affetto (test diagnostico), oppure a individuare o escludere la presenza di una mutazione associata ad una malattia genetica che possa svilupparsi in un individuo non affetto o, ancora, a valutare la maggiore o minore suscettibilità di un individuo a sviluppare malattie multifattoriali (test predittivo o di suscettibilità);
d) test farmacogenetico, il test genetico finalizzato all'identificazione di specifiche variazioni nella sequenza del Dna in grado di predire la risposta "individuale" a farmaci in termini di efficacia e di rischio relativo di eventi avversi;
e) test farmacogenomico, il test genetico finalizzato allo studio globale delle variazioni del genoma o dei suoi prodotti correlate alla scoperta di nuovi farmaci e all'ulteriore caratterizzazione dei farmaci autorizzati al commercio;
f) test sulla variabilità individuale, i test genetici che comprendono: il test di parentela volto alla definizione dei rapporti di parentela; il test ancestrale volto a stabilire i rapporti di una persona nei confronti di un antenato o di una determinata popolazione o quanto del suo genoma sia stato ereditato dagli antenati appartenenti a una particolare area geografica o gruppo etnico; il test di identificazione genetica volto a determinare la probabilità con la quale un campione o una traccia di DNA recuperato da un oggetto o altro materiale appartenga a una determinata persona;
g) screening genetico, il test genetico effettuato su popolazioni o su gruppi definiti, comprese le analisi familiari finalizzate a identificare -mediante "screening a cascata"- le persone potenzialmente a rischio di sviluppare la malattia genetica, al fine di delinearne le caratteristiche genetiche comuni o di identificare precocemente soggetti affetti o portatori di patologie genetiche o di altre caratteristiche ereditarie;

h) consulenza genetica, le attività di comunicazione volte ad aiutare l'individuo o la famiglia colpita da patologia genetica a comprendere le informazioni mediche che includono la diagnosi e il probabile decorso della malattia, le forme di assistenza disponibili, il contributo dell'ereditarietà al verificarsi della malattia, il rischio di ricorrenza esistente per sé e per altri familiari e l'opportunità di portarne a conoscenza questi ultimi, nonché tutte le opzioni esistenti nell'affrontare il rischio di malattia e l'impatto che tale rischio può avere su scelte procreative; nell'esecuzione di test genetici tale consulenza comprende inoltre informazioni sul significato, i limiti, l'attendibilità e la specificità del test nonché le implicazioni dei risultati; a tale processo partecipano, oltre al medico e/o al biologo specialisti in genetica medica, altre figure professionali competenti nella gestione delle problematiche psicologiche e sociali connesse alla genetica;

i) informazione genetica, le attività volte a fornire informazioni riguardanti le specifiche caratteristiche degli screening genetici.

Il prelievo e l'utilizzo dei campioni biologici e il trattamento dei dati genetici devono essere svolti secondo modalità volte a prevenire la violazione dei diritti, delle libertà fondamentali e della dignità degli interessati. Tali attività sono effettuate, comunque, in modo lecito e secondo correttezza, nonché per scopi determinati in conformità al presente regolamento e resi noti all'interessato nei modi indicati dal Nuovo Regolamento sulla protezione dei dati Personali UE/2016/679

Devono essere predisposte specifiche misure per accertare univocamente l'identità del soggetto al quale viene prelevato il materiale biologico per l'esecuzione dell'analisi.

Il trattamento dei dati genetici deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità. Restano fermi gli obblighi deontologici relativi alle singole figure professionali atte a svolgere tale attività.

18.1 – Raccolta e conservazione

La raccolta di dati genetici effettuata per l'esecuzione di test e di screening genetici è limitata alle sole informazioni personali e familiari strettamente indispensabili all'esecuzione dell'analisi. In particolare, nei trattamenti effettuati mediante test sulla variabilità individuale non sono raccolti dati sullo stato di salute o su altre caratteristiche degli interessati, ad eccezione del sesso. Il campione è prelevato da un incaricato del laboratorio di genetica medica o da un medico da esso designato.

18.2 – Ricerca scientifica e statistica

La ricerca scientifica e statistica, per il cui svolgimento è consentito il trattamento dei dati genetici e l'utilizzo dei campioni biologici, è effettuata, altresì, sulla base di un progetto redatto conformemente agli standard del pertinente settore disciplinare, anche al fine di documentare che il trattamento dei dati e l'utilizzo dei campioni biologici sia effettuato per idonei ed effettivi scopi scientifici. Possono essere utilizzati a tal fine i dati e i campioni biologici strettamente pertinenti agli scopi perseguiti, avuto riguardo ai dati disponibili e ai trattamenti già effettuati dallo stesso titolare, nonché all'esistenza di altre modalità che permettano di raggiungere gli scopi della ricerca mediante dati personali diversi da quelli identificativi o genetici, ovvero che non comportino il prelievo di campioni biologici.

Il progetto specifica le misure da adottare nel trattamento dei dati personali per garantire il rispetto della presente autorizzazione, nonché della normativa sulla protezione dei dati personali, anche per i profili riguardanti la custodia e la sicurezza dei dati e dei campioni biologici, e individua gli eventuali responsabili del trattamento. In particolare, laddove la

ricerca preveda il prelievo e/o l'utilizzo di campioni biologici, il progetto indica l'origine, la natura e le modalità di prelievo e di conservazione dei campioni, nonché le misure adottate per garantire la volontarietà del conferimento del materiale biologico da parte dell'interessato.

Il progetto è conservato a cura del titolare in forma riservata almeno per un anno dopo la conclusione della ricerca. Il titolare fornisce le informazioni contenute nel progetto agli interessati che ne facciano richiesta.

Quando le finalità della ricerca possono essere realizzate soltanto tramite l'identificazione anche temporanea degli interessati, il titolare adotta specifiche misure per mantenere separati i dati identificativi dai campioni biologici e dalle informazioni genetiche già al momento della raccolta, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o richieda un impiego di mezzi manifestamente sproporzionato.

18.3 – Misure di sicurezza

Per la custodia e la sicurezza dei dati genetici e dei campioni biologici sono adottate, in ogni caso, le seguenti cautele. L'accesso ai locali è controllato mediante incaricati della vigilanza o strumenti elettronici che prevedano specifiche procedure di identificazione anche mediante dispositivi biometrici. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

La conservazione, l'utilizzo e il trasporto dei campioni biologici sono posti in essere con modalità volte anche a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità.

Il trasferimento dei dati genetici in formato elettronico è effettuato con posta elettronica certificata previa cifratura delle informazioni trasmesse da realizzarsi con firma digitale. È ammesso il ricorso a canali di comunicazione di tipo "web application" che prevedano protocolli di comunicazione sicuri e garantiscano, previa verifica, l'identità digitale del server che eroga il servizio e della postazione client da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione.

La consultazione dei dati genetici trattati con strumenti elettronici è consentita previa adozione di sistemi di autenticazione basati sull'uso combinato di informazioni note agli incaricati e di dispositivi, anche biometrici, in loro possesso.

I dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero dei dati e dei campioni trattati, li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettano di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati siano tenuti con strumenti elettronici e contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate. Restano comunque fermi gli altri obblighi previsti dalla normativa vigente. Tali obblighi vanno osservati anche in riferimento ai campioni biologici.

18.4 –Informativa

L'informativa evidenzia, oltre agli elementi previsti dal Codice:

a) l'esplicitazione analitica di tutte le specifiche finalità perseguite;
b) i risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati genetici;
c) il diritto dell'interessato di opporsi al trattamento dei dati genetici per motivi legittimi;
d) la facoltà o meno, per l'interessato, di limitare l'ambito di comunicazione dei dati genetici e il trasferimento dei campioni biologici, nonché l'eventuale utilizzo di questi per ulteriori scopi;
e) il periodo di conservazione dei dati genetici e dei campioni biologici.

Nel caso in cui sia previsto il trasferimento di dati genetici e di campioni anche in Paesi non appartenenti all'Unione europea l'informativa deve specificare se tali Paesi non garantiscono un livello di tutela delle persone adeguato, nonché gli estremi identificativi dei soggetti destinatari dei dati e dei campioni, al fine di garantire in concreto all'interessato la possibilità di esercitare il controllo sui dati e sui campioni che lo riguardano.

Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini dell'acquisizione di una nuova manifestazione del consenso quando questo è necessario.

Per i trattamenti effettuati per scopi di ricerca scientifica e statistica l'informativa evidenzia, altresì:

a) che il consenso è manifestato liberamente ed è revocabile in ogni momento senza che ciò comporti alcuno svantaggio o pregiudizio per l'interessato, salvo che i dati e i campioni biologici, in origine o a seguito di trattamento, non consentano più di identificare il medesimo interessato;
b) gli accorgimenti adottati per consentire l'identificabilità degli interessati soltanto per il tempo necessario agli scopi della raccolta o del successivo trattamento;
c) l'eventualità che i dati e/o i campioni biologici siano conservati e utilizzati per altri scopi di ricerca scientifica e statistica, per quanto noto, adeguatamente specificati anche con riguardo alle categorie di soggetti ai quali possono essere eventualmente comunicati i dati oppure trasferiti i campioni;
d) le modalità con cui gli interessati che ne facciano richiesta possono accedere alle informazioni contenute nel progetto di ricerca.

Per i trattamenti effettuati mediante test e screening genetici per finalità di tutela della salute, di ricerca o di ricongiungimento familiare, l'informativa è resa all'interessato prima del prelievo, ovvero dell'utilizzo del suo campione biologico qualora lo stesso sia stato già prelevato, anche in forma scritta, in modo specifico e comprensibile, anche quando il trattamento è effettuato da esercenti la professione sanitaria o da organismi sanitari pubblici e privati che abbiano informato in precedenza il medesimo interessato utilizzando le modalità semplificate previste dalla normativa vigente.

I trattamenti per lo svolgimento delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria possono essere effettuati mediante l'esecuzione di test genetici soltanto previa informativa all'interessato da rendersi con le modalità sopra indicate.

18.5 – Consulenza genetica e attività di informazione

Per i trattamenti effettuati mediante test genetici per finalità di tutela della salute o di ricongiungimento familiare è fornita all'interessato una consulenza genetica prima e dopo lo svolgimento dell'analisi. Prima dell'introduzione di screening genetici finalizzati alla tutela della salute da parte di organismi sanitari sono adottate idonee misure per garantire un'attività di

informazione al pubblico in merito alla disponibilità e alla volontarietà dei test effettuati, alle specifiche finalità e conseguenze, anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica.

Il consulente genetista aiuta i soggetti interessati a prendere in piena autonomia le decisioni ritenute più adeguate, tenuto conto del rischio genetico, delle aspirazioni familiari e dei loro principi etico-religiosi, aiutandoli ad agire coerentemente con le scelte compiute, nonché a realizzare il miglior adattamento possibile alla malattia e/o al rischio di ricorrenza della malattia stessa.

Sono adottate cautele idonee ad evitare che la consulenza genetica avvenga in situazioni di promiscuità derivanti dalle modalità utilizzate o dai locali prescelti, nonché a prevenire l'indebita conoscenza da parte di terzi di informazioni genetiche o idonee a rivelare lo stato di salute.

Nei casi in cui il test sulla variabilità individuale è volto ad accertare la paternità o la maternità gli interessati sono, altresì, informati circa la normativa in materia di filiazione, ponendo in evidenza le eventuali conseguenze psicologiche e sociali dell'esame.

L'attuazione di ricerche scientifiche su isolati di popolazione è preceduta da un'attività di informazione presso le comunità interessate, anche mediante mezzi di comunicazione di massa su base locale e presentazioni pubbliche, volta ad illustrare la natura della ricerca, le finalità perseguite, le modalità di attuazione, le fonti di finanziamento e i rischi o benefici attesi per le popolazioni coinvolte. L'attività di informazione evidenzia anche gli eventuali rischi di discriminazione o stigmatizzazione delle comunità interessate, nonché quelli inerenti alla conoscibilità di inattesi rapporti di consanguineità e le azioni intraprese per ridurre al minimo tali rischi.

18.6 – Consenso

In conformità a quanto previsto dalla normativa, i dati genetici possono essere trattati e i campioni biologici utilizzati soltanto per gli scopi indicati nella presente regolamento e rispetto ai quali la persona abbia manifestato previamente e per iscritto il proprio consenso informato. Il consenso resta valido solo se l'interessato è libero da ogni condizionamento o coercizione e resta revocabile liberamente in ogni momento. Nel caso in cui l'interessato revochi il consenso al trattamento dei dati per scopi di ricerca, è distrutto anche il campione biologico sempre che sia stato prelevato per tali scopi, salvo che, in origine o a seguito di trattamento, il campione non possa più essere riferito ad una persona identificata o identificabile.

Per i trattamenti effettuati mediante test genetici, compreso lo screening, anche a fini di ricerca o di ricongiungimento familiare, deve essere acquisito il consenso informato dei soggetti cui viene prelevato il materiale biologico necessario all'esecuzione dell'analisi. In questi casi, all'interessato è richiesto di dichiarare se vuole conoscere o meno i risultati dell'esame o della ricerca, comprese eventuali notizie inattese che lo riguardano, qualora queste ultime rappresentino per l'interessato un beneficio concreto e diretto in termini di terapia o di prevenzione o di consapevolezza delle scelte riproduttive.

Per le informazioni relative ai nascituri il consenso è validamente prestato dalla gestante. Nel caso in cui il trattamento effettuato mediante test prenatale possa rivelare anche dati genetici relativi alla futura insorgenza di una patologia del padre, è previamente acquisito anche il consenso di quest'ultimo.

Quando il trattamento è necessario per la salvaguardia della vita e dell'incolumità fisica dell'interessato, e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, incapacità d'agire o incapacità di intendere o di volere, il consenso è manifestato 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'opinione del minore, nella misura in cui lo consente la sua età e il suo grado di maturità, è, ove possibile, presa in considerazione, restando preminente in ogni caso l'interesse del minore. Negli altri casi di incapacità, il trattamento è consentito se le finalità perseguite comportano un beneficio diretto per l'interessato e la sua opinione è, ove possibile, presa in considerazione, restando preminente in ogni caso l'interesse dell'incapace.

I dati e i campioni biologici di persone che non possono fornire il proprio consenso per incapacità, possono essere trattati per finalità di ricerca scientifica che non comportino un beneficio diretto per i medesimi interessati qualora ricorrano contemporaneamente le seguenti condizioni:

a) la ricerca è finalizzata al miglioramento della salute di altre persone appartenenti allo stesso gruppo d'età o che soffrono della stessa patologia o che si trovano nelle stesse condizioni e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale;
b) una ricerca di analoga finalità non può essere realizzata mediante il trattamento di dati riferiti a persone che possono prestare il proprio consenso;
c) il consenso al trattamento è acquisito 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;
d) la ricerca non comporta rischi significativi per la dignità, i diritti e le libertà fondamentali degli interessati.

In tali casi, resta fermo quanto sopra previsto in ordine all'esigenza di tenere in considerazione, ove possibile, l'opinione del minore o dell'incapace.

I trattamenti di dati connessi all'esecuzione di test genetici presintomatici possono essere effettuati sui minori non affetti, ma a rischio per patologie genetiche solo nel caso in cui esistano concrete possibilità di terapie o di trattamenti preventivi prima del raggiungimento della maggiore età. I test sulla variabilità individuale non possono essere condotti su minori senza che venga acquisito il consenso di ambedue i genitori, ove esercitano entrambi la potestà sul minore.

I trattamenti di dati connessi all'esecuzione di test genetici per lo svolgimento delle investigazioni difensive o per l'esercizio di un diritto in sede giudiziaria possono essere effettuati soltanto con il consenso informato della persona cui appartiene il materiale biologico necessario all'indagine, salvo che un'espressa disposizione di legge, o un provvedimento dell'autorità giudiziaria in conformità alla legge, disponga altrimenti.

18.7 – Comunicazione e diffusione dei dati

I dati genetici non possono essere comunicati e i campioni biologici non possono essere messi a disposizione di terzi salvo che sia indispensabile per il perseguimento delle finalità indicate dall'Autorizzazione generale al trattamento dei dati genetici - 24 giugno 2011 *(Pubblicato sulla Gazzetta Ufficiale n. 159 dell'11 luglio 2011).*

I dati genetici e i campioni biologici raccolti per scopi di ricerca scientifica e statistica possono essere comunicati o trasferiti a enti e istituti di ricerca, alle associazioni e agli altri organismi pubblici e privati aventi finalità di ricerca, esclusivamente nell'ambito di progetti congiunti.

I dati genetici e i campioni biologici raccolti per scopi di ricerca scientifica e statistica possono essere comunicati o trasferiti ai soggetti sopra indicati, non partecipanti a progetti congiunti, limitatamente alle informazioni prive di dati identificativi, per scopi scientifici direttamente collegati a quelli per i quali sono stati originariamente raccolti e chiaramente determinati per iscritto nella richiesta dei dati e/o dei campioni. In tal caso, il soggetto richiedente si impegna a non trattare i dati e/o utilizzare i campioni per fini diversi da quelli indicati nella richiesta e a non comunicarli o trasferirli ulteriormente a terzi.

I dati genetici raccolti a fini di ricongiungimento familiare possono essere comunicati unicamente alle rappresentanze diplomatiche o consolari competenti all'esame della documentazione prodotta dall'interessato o all'organismo internazionale ritenuto idoneo dal Ministero degli affari esteri cui questi si sia rivolto. I campioni biologici prelevati ai medesimi fini possono essere trasferiti unicamente al laboratorio designato per l'effettuazione del test sulla variabilità individuale o all'organismo internazionale ritenuto idoneo dal Ministero degli affari esteri.

I dati genetici devono essere resi noti di regola direttamente all'interessato o a persone diverse dal diretto interessato sulla base di una delega scritta di quest'ultimo, adottando ogni mezzo idoneo a prevenire la conoscenza non autorizzata da parte di soggetti anche compresenti. La comunicazione nelle mani di un delegato dell'interessato è eseguita in plico chiuso.

Gli esiti di test e di screening genetici, nonché i risultati delle ricerche qualora comportino per l'interessato un beneficio concreto e diretto in termini di terapia, prevenzione o di consapevolezza delle scelte riproduttive, devono essere comunicati al medesimo interessato anche nel rispetto della sua dichiarazione di volontà di conoscere o meno tali eventi e, ove necessario, con un'appropriata consulenza genetica.

Gli esiti di test e di *screening* genetici, nonché i risultati delle ricerche, qualora comportino un beneficio concreto e diretto in termini di terapia, prevenzione o di consapevolezza delle scelte riproduttive, anche per gli appartenenti alla stessa linea genetica dell'interessato, possono essere comunicati a questi ultimi, su loro richiesta, qualora l'interessato vi abbia espressamente acconsentito oppure qualora tali risultati siano indispensabili per evitare un pregiudizio per la loro salute, ivi compreso il rischio riproduttivo, e il consenso dell'interessato non sia prestato o non possa essere prestato per effettiva irreperibilità.

In caso di ricerche condotte su popolazioni isolate, devono essere resi noti alle comunità interessate e alle autorità locali gli eventuali risultati della ricerca che rivestono un'importanza terapeutica o preventiva per la tutela della salute delle persone appartenenti a tali comunità.

I dati genetici non possono essere diffusi. I risultati delle ricerche non possono essere diffusi se non in forma aggregata, ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti, anche nell'ambito di pubblicazioni.

ART. 19 - Medico competente

Nell'azienda vi possono essere dipendenti sottoposti a sorveglianza sanitaria in base alla normativa vigente.

Per questi dipendenti è quindi opportuno che il consenso informato comprenda anche questo particolare trattamento di dati (anche sensibili) compiuto dal medico competente.

Qualora non si voglia utilizzare il modello generale di consenso informato per i dipendenti, ma si preferisca separare questo consenso informato, si può utilizzare un modello che dovrà essere predisposto direttamente dal medico competente qualora egli adempia agli obblighi previsti dalla normativa sulla sicurezza nella gestione di un contratto di somministrazione di lavoro di cui agli artt. 20 e ss del d.lgs.vo. 276/2003

ART. 20 – Consenso informato e tutela della riservatezza nell'accertamento dell'infezione HIV

Il consenso informato ai trattamenti sanitari e la tutela della riservatezza dei dati personali rappresentano due importanti applicazioni del principio dell'autonomia, che richiede quindi:

- che gli individui vengano trattati come soggetti autonomi e che quindi le loro preferenze siano rispettate e che la loro partecipazione decisionale venga suscitata e tutelata;

- l'operatore sanitario e ogni altro soggetto che viene a conoscenza di un caso di AIDS, ovvero di un caso di infezione da HIV, anche non accompagnato da stato morboso, è tenuto a prestare la necessaria assistenza e ad adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato, nonché della relativa dignità;

- La rilevazione statistica della infezione da HIV deve essere comunque effettuata con modalità che non consentano l'identificazione della persona;

- sono consentite analisi di accertamento dell'infezione da HIV, nell'ambito di programmi epidemiologici, soltanto quando i campioni da analizzare siano stati resi anonimi con assoluta impossibilità di pervenire alla identificazione delle persone interessate;

- le operazioni di raccolta dei dati relativi al paziente nonché la circolazione della documentazione sanitaria nel reparto devono essere presidiate dalla garanzia di *una adeguata selezione dei dati da riportare in cartella, limitandosi a quelli di effettivo interesse per la tutela della salute del paziente* oltre che *dal rafforzamento del dovere deontologico di tenuta di condotte adeguate alla tutela della riservatezza*

- come previsto dalla legge 5 giugno 1990, n. 135 in tema di Aids e HIV la comunicazione di risultati di accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti. Tale disposizione, in particolare, consentirebbe anche di evitare che il paziente venga a conoscenza dei dati da parte di terzi e, d'altra parte, di prevenire il pericolo di discriminazione ed emarginazione del sieropositivo;

È onere del personale sanitario, dei Responsabili e degli incaricati al trattamento dimostrare di avere adottato tutte le misure idonee allo scopo di garantire il diritto del paziente alla riservatezza e di evitare che i dati relativi all'esito del test e alle condizioni di salute del paziente medesimo possano pervenire a conoscenza di terzi.

ART. 21 – Misure per il rispetto degli interessati

Presso i locali dell'Azienda, a cura di ciascun Responsabile del trattamento dati, sono, adottate misure idonee ad assicurare che le informazioni sanitarie, rese agli utenti verbalmente (chiamata dei pazienti, indagine anamnestica, elaborazione diagnostica, colloqui con i familiari ecc.) o tramite supporto cartaceo (documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati.

Le procedure informatiche installate devono essere configurate in modo da mettere in atto misure tecnologiche e organizzative adeguate ed efficaci per dimostrare la conformità delle attività con la normativa vigente. In particolare devono garantire la corretta gestione dei consensi tramite l'utilizzo di supporti tecnologi, che permettano la storicizzazione della volontà espressa dal paziente di trattare o meno i dati forniti e renderli disponibili.

ART. 22 – Amministratore di Sistema

L'Amministratore di sistema è individuato con apposito atto scritto del Direttore Generale. Costui avrà il compito di generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, la parola chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dei dati, nel rispetto delle massime misure di Sicurezza.

Dovrà adottare idonee misure di sicurezza atte a garantire la protezione degli strumenti software e hardware, utilizzando le conoscenze acquisite in base al progresso tecnologico.

Lo stesso avrà il compito di controllare periodicamente l'efficienza dei sistemi tecnici adottati e di redigere apposita relazione, da consegnare al titolare, riportante i riscontri e le verifiche effettuate, i parametri adottati e gli accorgimenti proposti per migliorare la Sicurezza.

Oltre le misure idonee, restano consigliate le seguenti attività:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di backup;
- assicurarsi della qualità delle copie di backup dei dati e della loro conservazione in luogo adatto e sicuro;
- fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USERID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali, per oltre sei mesi;
- fornire un Report annuale, per quanto sopra specificato, fornendo le proprie indicazioni e suggerimenti;
- E, altresì, compito dell'Amministratore di sistema indicare al personale competente o provvedere direttamente alla distruzione o allo smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego.

ART. 23 – Formazione del personale

Quando necessario, l'Azienda organizza nell'ambito dei programmi di formazione continua del personale interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali, finalizzati alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi.

ART. 24 – Procedure organizzative a tutela della riservatezza in ambito sanitario

Presso tutti i presidi dell'Azienda, a cura del dirigente del presidio medesimo, sono adottate procedure, quali:

- l'adozione di opportuna segnaletica per delimitare le distanze di cortesia, atte a garantire la riservatezza degli utenti in occasione di richiesta o fruizione di prestazioni sanitarie (prenotazioni, esami diagnostici, visite mediche, certificazioni, etc.) o amministrative (rimborsi, indennità, ecc.).
- I Responsabili dei trattamenti sono tenuti ad adottare idonee misure atte a garantire che le informazioni sanitarie personali rese agli utenti verbalmente (es.: chiamata dei pazienti, Indagine anamnestica, elaborazione diagnostica, colloqui con familiari, ecc.) o tramite supporto cartaceo (es.: documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati.
- Le strutture ospedaliere non possono fornire informazioni sui degenti, la loro presenza in ospedale e loro collocazione all'interno della struttura, se non è stata preventivamente acquisita specifica autorizzazione dagli interessati ed indicazione delle persone cui desiderano indirizzare o meno dette notizie.
- Non possono essere esposti al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati.

ART. 25 – Pubblicità degli atti e diritto alla riservatezza

Salva diversa disposizione di legge, l'Azienda garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo delle deliberazioni o di alti atti, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati. Per assicurare comunque la completezza delle deliberazioni, i dati personali da escludere dalla pubblicazione sono inseriti nell'originale integrale del documento, che viene trattenuto agli atti e il cui accesso è consentito nei casi e con le modalità di cui all'Art. 20.

ART. 26 – Diritto di accesso alla documentazione

Salvo quanto previsto dal Regolamento Europeo (*UE/2016/679)* e fatti salvi gli atti sottratti all'accesso per norma di legge, l'Azienda garantisce il diritto di accesso alla documentazione amministrativa a chiunque abbia un interesse personale e concreto per la tutela di situazioni giuridicamente rilevanti, nonché nell'esercizio dello svolgimento delle investigazioni difensive di cui agli artt. 327 bis e seguenti c.p.p., nonché secondo quanto stabilito dal Regolamento del diritto di accesso agli atti amministrativi adottato dall'Azienda.

Nel caso l'istanza di accesso riguardi documentazione contenente dati personali, comuni o sensibili, di terzi, l'accesso è

limitato alla sola visione dei dati la cui conoscenza sia necessaria per curare o difendere un proprio interesse giuridico, nel rispetto dei principi di pertinenza e di non eccedenza dei dati da visionare rispetto alle finalità per le quali è consentito l'accesso stesso. Qualora l'istanza di accesso riguardi documenti contenenti dati idonei a rivelare lo stato di salute o la vita sessuale di un terzo, l'accesso è consentito a condizione che ciò si renda necessario per far valere o difendere in sede giudiziaria una situazione giuridicamente rilevante di rango almeno pari ai diritti del terzo, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso stesso.

È comunque garantito l'accesso agli atti amministrativi che non contengono dati personali di soggetti diversi da quelli del richiedente, sempreché ricorrano i presupposti previsti dall'articolo 22 della legge 7 agosto 1990, n. 241 e s.i.m., e dall'articolo 2 del D.P.R. 27 giugno 1992, n. 352 e s.i.m.

Per l'attuazione del presente Regolamento l'Azienda adotta appositi modelli, in collaborazione con i Responsabili del trattamento interessati. Eventuali ulteriori modelli da adottare per specifiche esigenze organizzative delle strutture sono predisposti dai Responsabili del trattamento, in relazione alle rispettive competenze, con verifica del contenuto da parte dell'Ufficio Privacy.

ART. 27 – Misure di sicurezza

Per "misure di sicurezza" deve intendersi l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un idoneo livello di sicurezza nel trattamento dei dati.

27.1 Criteri tecnici ed organizzativi per la protezione delle aree e dei locali

I dati e le informazioni di carattere sensibile e/o giudiziario devono essere trattati in aree protette - anche fisicamente - dall'accesso di persone non autorizzate. Sono perciò individuati spazi, dotati di un sistema di controllo all'ingresso e di eventuali sbarramenti di sicurezza. Un livello di protezione più elevato deve essere attivato per gli ambiti di trattamento e/o conservazione dei dati sensibili e giudiziari e ove sono ubicati i server di residenza dei dati e delle informazioni. Le barriere fisiche, dove necessario, devono essere configurate in modo tale da impedire l'accesso alle persone non autorizzate. Quando restano vuote, le aree di sicurezza devono essere chiuse.

Il personale in servizio presso l'Azienda ha accesso ai locali esclusivamente per l'adempimento della prestazione lavorativa.

Il personale che espleta servizi strumentali (es.: pulizia dei locali) o si occupa della manutenzione e dei servizi accessori, deve essere espressamente autorizzato ad accedere alle aree di sicurezza.

L'assegnazione degli spazi di lavoro deve avvenire secondo criteri tali da impedire la promiscuità di permanenza e di utilizzazione tra:

personale incaricato del trattamento di dati personali; personale non incaricato di trattamento di dati personali; soggetti

estranei all'Azienda.

Il personale dipendente incaricato del trattamento ha accesso ai dati esclusivamente sulla base delle esigenze di servizio, conformemente ai seguenti principi:

- la necessità di trattamento;
- il minimo livello di conoscenza dei dati.

Responsabili del trattamento devono vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari.

È altresì compito del Responsabile vigilare sull'introduzione in tali aree di oggetti, apparecchiature, sostanze o materiali che possono favorire il sorgere di rischi. Devono essere previsti procedure, accorgimenti e strumenti per:

- consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale autorizzato, ivi compresi i locali destinati al personale addetto alla video sorveglianza;
- ostacolare l'accesso abusivo ai dati; segnalare la presenza di intrusi;

27.2 Attività svolte a livello centrale

L'uscita verso la rete internet di tutti i collegamenti aziendali, è concentrata in un unico nodo principale. Questo punto, chiamato tecnicamente "centro stella", raccoglie tutte le apparecchiature hardware ed i sistemi di tracciamento atti a verificare la correttezza dei collegamenti secondo i principi di:

- **riservatezza:** prevenzione contro l'accesso non autorizzato alle informazioni
- **integrità:** le informazioni non devono essere alterabili da incidenti o abusi
- **disponibilità dei dati:** il sistema deve essere protetto da interruzioni impreviste

Il governo di un'infrastruttura complessa ed articolata come quella in oggetto per soddisfare le esigenze precedentemente espresse nonché l'adeguamento della rete alle norme in materia di trattamento dei dati personali, rende necessaria l'implementazione di una piattaforma di tipo **"protocollo AAA"**. È un protocollo che realizza le tre funzioni di autenticazione (***authentication***), controllo degli accessi (***authorization***) e tracciamento del consumo delle risorse da parte degli utenti (***accounting***). L'espressione "protocollo AAA" non si riferisce dunque a un particolare protocollo ma a una famiglia di protocolli che offrono, anche in modi diversi, i servizi di autenticazione (*authentication*), controllo degli accessi (*authorization*) e tracciamento delle attività degli utenti relative all'infrastruttura ed ai servizi da essa veicolati (*accounting*). Tale infrastruttura, inoltre, fornisce all'Azienda diritti e strumenti di "provisioning" estese a tutte le risorse esistenti, ovvero utenti, PDL (Postazioni Di Lavoro), stampanti, servizi di rete, servizi applicativi, etc.

L'implementazione di un "Dominio" risulta fondamentale per l'attuazione della sicurezza e dovrà essere di tipo a struttura centralizzata e dotato di un elevato livello di ridondanza delle componenti critiche.

Tramite gli strumenti di amministrazione di Windows, si potrà procedere alla definizione ed applicazione delle policy di sicurezza all'interno del dominio, relativamente ai privilegi operativi dell'utenza e alla gestione della configurazione delle postazioni di lavoro, integrandole con tutti gli aspetti di gestione della sicurezza aziendale.

L'attivazione e la gestione delle policy di domino Active Directory, permetterà di definire dei criteri di profilazione operativa di utenti e risorse e rende possibile tracciare, controllare e gestire l'intero ciclo di vita aziendale delle risorse secondo criteri conformi alle normative di riferimento.

L'utenza della rete accede oggi ai servizi Internet tramite due accessi distinti: uno installato presso la sede Garibaldi Centro un altro presso Garibaldi Nesima, attualmente quindi:

- Tutti gli utenti possono accedere ad internet, se autorizzati;
- Il servizio di accesso profila i diritti di accesso verso internet del singolo utente o del gruppo di utenti;
- Tutte le attività svolte dallo stesso, sono registrate tramite file di log, affinché su eventuale richiesta degli organi competenti, possa essere documentata l'attività del singolo utente per periodo temporale, per tipologia di servizio, o per destinazione Internet raggiunta;
- L'accesso ad Internet, oltre ad essere regolamentato, si può definire "sicuro" ovvero è stato filtrato il traffico in ingresso ed in uscita al fine di:
    - Impedire l'accesso a siti internet i cui contenuti non sono direttamente assimilabili all'attività istituzionale;
    - Impedire il download o l'upload di contenuti non istituzionali;
    - Effettuare il filtraggio di contenuti potenzialmente pericolosi, es. Virus, spyware, malware, adware, etc;

  Nel centro stella sono presenti apparati che controllano gli accessi da e verso internet.

27.3 Comportamenti e regole a cui bisogna attenersi

Chiudere a chiave cassetti ed uffici

Per evitare che persone non autorizzate accedano ai dati, il primo livello di protezione è sicuramente quello fisico, ed un cassetto od una porta chiusi a chiave sono sicuramente ostacoli non banali per chi vuole accedere a dei dati. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e leggere i documenti posti su una scrivania o visibili su uno schermo. Si richiede pertanto, ove necessario, di chiudere a chiave cassetti e uffici in caso di assenza prolungata e prima di lasciare il posto di lavoro a fine giornata e per la pausa pranzo.

Conservare supporti di memoria e stampe in luoghi sicuri.

Alla conservazione dei supporti di memoria (DVD, CD, etc.) si applicano gli stessi criteri di protezione dei documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. Come il personale ha l'accortezza di non lasciare importanti documenti alla portata di sguardi indiscreti, così deve comportarsi con supporti di memoria e stampe contenenti dati riservati. Il personale deve riporre tali supporti sotto chiave non appena terminato il loro utilizzo.

Stampe di documenti riservati

Per stampe riservate deve essere evitato l'utilizzo di periferiche di rete, in quanto le informazioni potrebbero essere intercettate da altre persone sia fisicamente che per mezzo di appositi programmi; se è indispensabile l'utilizzo di tali periferiche, usare almeno la modalità di stampa ritardata impostando un tempo sufficiente per raggiungere la stampante prima che inizi il suo lavoro. Le stampe devono essere ritirate appena prodotte e non devono essere lasciate sulle stampanti, soprattutto su quelle di rete.

Non gettare nel cestino stampe di documenti che possono contenere informazioni confidenziali

Se si trattano dati di particolare riservatezza, si consideri la possibilità di dotarsi di una macchina distruggi-documenti (shredder) per l'eliminazione di stampe non più necessarie. In particolare è possibile che l'utente effettui varie copie di stampe prima di ottenerne una che lo soddisfi: soprattutto se il documento contiene dati riservati, distruggere personalmente le copie non utilizzate.

Non lasciare lavori incompiuti sullo schermo

Si deve avere l'accortezza di non lasciare lavori incompiuti sullo schermo e chiudere le applicazioni quando si lascia il posto di lavoro; l'assenza potrebbe essere maggiore del previsto e bisogna considerare che un documento presente sullo schermo ha la caratteristica di attirare la curiosità delle persone.

Spegnere il computer se ci si assenta per un periodo di tempo lungo

Lasciare un computer acceso non crea problemi al suo funzionamento e velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza, maggiore è la probabilità che nel frattempo avvenga un'interruzione dell'energia elettrica che possa portare un danno all'elaboratore, alla sua configurazione o al documento stesso.

Proteggere attentamente i dati.

Bisogna prestare particolare attenzione ai dati importanti, di cui si è comunque personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare tutti i dati come se fossero importanti. Come minimo proteggerli con password e non dare a nessun altro utente il permesso di accesso (lettura o modifica).

Manutenzione Hardware e Software

Ove possibile, tutti i PC sono stati dotati di una installazione di base che comprende vari software. Non è permesso modificare o rimuovere queste installazioni. Nel caso in cui sia necessaria la modifica di questo ambiente, tale intervento deve essere richiesto al Servizio Informatica ed eseguito solo dopo autorizzazione scritta.

Impostare il salvaschermo

È importante impostare il salvaschermo con richiesta di password per poter riprendere il controllo della postazione; in tal modo se ci si assenta per alcuni minuti dal proprio posto di lavoro, il PC diviene inutilizzabile.

Abilitare l'accesso tramite password, ove possibile.

Gli applicativi come WORD ed EXCEL permettono di proteggere i propri dati tramite password. Imparare a utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

Account di accesso

L'accesso ai Server o in generale al dominio, come quello di ogni programma critico, richiede di identificarsi a mezzo di un nome utente ed una password. Le operazioni vengono registrate (file di LOG) tenendo traccia dell'utente che le ha eseguite e quindi in base all'account utilizzato. Ogni utente deve avere l'accortezza di non permettere ad altri di utilizzare le proprie chiavi di accesso, anche per non rendersi responsabile di operazioni non eseguite personalmente. Nel caso si stia utilizzando una stazione di lavoro e si intenda passare a lavorare su una differente, l'utente è tenuto a chiudere le applicazioni e le sessioni di lavoro aperte sul suo computer ed autenticarsi sull'altro sempre con le proprie credenziali. A tal fine è stata disabilitata, ove possibile, la funzionalità che permetta di utilizzare le stesse chiavi di accesso da più di un computer alla volta.

Uso di computer ed account per personale esterno

La consultazione dei sistemi da parte di personale esterno in generale non deve essere permessa. Nel caso che personale esterno debba installare del nuovo software o hardware (schede o apparecchiature) sulla postazione di lavoro di un utente, l'operazione deve essere permessa solo in presenza dello stesso utente.

Condivisioni

Al fine di limitare la diffusione di virus, furti e danneggiamenti di documenti, problemi di funzionamento delle stazioni di lavoro, è fatto espressamente divieto di condividere il disco fisso del proprio computer o anche solo parte di esso. Nel caso vi siano delle esigenze di condividere documenti e/o dati, deve essere fatto presente al Responsabile che, con l'Amministratore di sistema, provvederà ad analizzare il problema e, qualora possibile e consentito dalle normative vigenti, verrà creata una apposita area di scambio con le opportune protezioni.

Accesso remoto sulla macchina (PC) per teleassistenza

Per ottimizzare i tempi di intervento e ridurre i relativi costi, è possibile che il Servizio Informatica richieda all'utente il permesso di accedere al PC. Solo dopo avere ottenuto dall'utente l'autorizzazione, il personale del Servizio Informatica potrà connettersi in teleassistenza per svolgere le attività che il caso richiede.

Usare il salvataggio automatico dei dati

Molti programmi applicativi, WORD ed EXCEL, consentono di salvare automaticamente il lavoro a intervalli fissi di tempo, in modo da minimizzare il rischio di perdita di dati in caso di guasti, mancanze di corrente, errori di programma. L'utente deve verificare se tale funzionalità sia possibile sui programmi utilizzati e, nel caso, verificare

che sia attiva; comunque salvare manualmente il proprio lavoro frequentemente e prendere l'abitudine di gestire i propri dati senza fare esclusivo affidamento sul sistema.

Effettuare salvataggi dei dati e conservare le copie in un luogo sicuro

Nel caso si presentassero dei mal funzionamenti dell'elaboratore e fosse necessaria una sua nuova installazione o una sua sostituzione, oppure anche la sola sostituzione del suo disco fisso interno, il personale informatico riesce a ripristinare la funzionalità di tutti i programmi autorizzati procedendo con delle nuove installazioni: può accadere che non sia in grado di recuperare i dati e/o documenti che erano presenti prima del guasto, come pure le personalizzazioni effettuate dall'utente. È fondamentale che ogni utente salvi i propri documenti critici ma non sensibili, anche su altri supporti fisici (CD, DVD, PenDrive); tali copie dovranno essere tenute chiuse a chiave in armadi possibilmente blindati e ignifughi collocati in un luogo differente rispetto a quello dove risiede l'elaboratore; quest'ultima accortezza è utile soprattutto in caso di incendio: più le copie di sicurezza sono distanti dall'elaboratore e meno è probabile che vengano distrutte con esso.

Utilizzo di access point wireless

Il loro utilizzo è generalmente vietato e autorizzabile solo in presenza di un adeguato livello di crittografia (chiave WEP). Con tali apparecchi, si può creare un punto di accesso non controllato e aperto al mondo esterno, che può rendere maggiormente vulnerabile non solo le postazioni di lavoro su cui sono collegate, ma l'intera rete. L'installazione, ove indispensabile, deve essere eseguita a cura del personale tecnico, ed esclusivamente a seguito di autorizzazione espressamente approvata per iscritto dal Servizio Informatica, previa autorizzazione del Responsabile del Servizio Informatica che certifichi l'impossibilità di raggiungere i medesimi obiettivi in modi maggiormente sicuri.

Altre apparecchiature

È fatto divieto agli utenti di collegare, o permettere ad altri di farlo, qualsiasi tipo di apparecchiatura sulle porte seriali, parallele, USB, etc. di qualsiasi elaboratore o apparato di rete. È permessa l'installazione solo dei kit per la firma digitale e di stampanti purché non siano collegate, in alcun modo, a linee telefoniche (ad es: stampanti multifunzioni, fax).

Fonti di dati, uso di internet

Gli utenti devono utilizzare i computer in dotazione per assolvere il proprio lavoro e devono pertanto utilizzarli per accedere ad informazioni inerenti le proprie mansioni. Non si devono quindi copiare o "scaricare" programmi, file musicali, immagini con contenuti pornografici, etc. dalla rete internet o da altre fonti. Non si debbono visitare siti illegali (ad esempio depositi di software pirata) che sono spesso usati come "specchietto per le allodole" per attirare visitatori su cui condurre attacchi informatici.

Posta elettronica

L'indirizzo di posta elettronica configurato per l'utente è uno strumento di lavoro e pertanto non può essere utilizzato per corrispondenza personale.

Dati e programmi provenienti dall'esterno

Come per la posta elettronica, è buona norma diffidare di tutti i dati e programmi che si ricevono, anche se la fonte appare affidabile o il contenuto molto interessante.

Provenienza dei computer e linee telefoniche

Possono essere utilizzati solo computer da tavolo e portatili di proprietà dell'Azienda o avere autorizzazione del Dirigente; possono essere collegati alla rete locale solo i computer che sono stati opportunamente configurati dal personale informatico aziendale e, per tutto il tempo in cui sono connessi alla rete locale, devono essere utilizzati esclusivamente da dipendenti.

Utilizzo di computer portatili

I PC portatili sono un facile bersaglio per i ladri quindi, se si ha la necessità di gestire dati riservati su di essi, questi devono essere protetti con almeno le password di BIOS e programmi di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto); deve inoltre essere effettuato periodicamente il salvataggio dei dati.

Uso di altri computer

Il personale NON deve permettere, a persone non dipendenti, il collegamento dei propri computer, anche se portatili, o altri apparati elettronici di qualsiasi natura, sia alle reti fonia/dati che ai computer in dotazione presso questi uffici, nonostante ci sia un motivo apparentemente valido. In tale modo si cercano di limitare i rischi relativi a conflitti di configurazioni ed alle intercettazioni di comunicazione e dati.

Installazioni di nuovi programmi

E' fatto divieto agli utenti di installare qualsiasi tipo di software, in particolar modo giochi e programmi che permettano condivisioni di file. Tutte le installazioni di programmi devono essere effettuate esclusivamente a cura o con l'ausilio del personale tecnico del Servizio Informatica e comunque richieste ed autorizzate dall'Amministrazione, in quanto le licenze di utilizzo dei programmi devono essere conteggiate e, se necessario, acquistate. Il personale che dovesse trasgredire tali norme, si assume la responsabilità personalmente per i danni eventualmente arrecati sia per la non osservanza delle regole sul copyright che per i danni provocati sulla rete. I responsabili delle UU.OO. sono invitati a mettere in atto ogni misura di vigilanza e di controllo affinché gli operatori osservino le disposizioni sopra impartite allo scopo di evitare, oltre che l'applicazione delle sanzioni previste dalla normativa vigente, l'adozione delle correlate misure disciplinari. Nel raccomandare la puntuale osservanza di quanto contenute nella presente disposizione, si rende noto che:

Il datore di lavoro ***ha la facoltà di effettuare controlli mirati*** – nel rispetto della libertà e della dignità dei lavoratori e comunicando in anticipo ai propri dipendenti le modalità.

Correzioni su archivi

Gli utenti sono tenuti a correggere personalmente i dati negli archivi, utilizzando le maschere degli applicativi rilasciati; nel caso questo non sia possibile e sia necessario un intervento di personale informatico, deve essere presentata apposita richiesta recante il problema e l'intervento proposto nei suoi dettagli; l'utente è tenuto a controllare personalmente il tecnico e l'esito del suo intervento.

Stampa di riepiloghi e statistiche

Gli utenti sono tenuti ad utilizzare solo i programmi Aziendali in dotazione, anche per produrre riepiloghi e stampe di qualsiasi natura, in quanto gli stessi sono stati testati. Nel caso si richieda ai tecnici di produrre altre stampe, si è tenuti ad affiancarli, controllandone l'operato.

Non violare le leggi in materia di sicurezza informatica

Ricordarsi che anche solo un tentativo di ingresso non autorizzato in un sistema costituisce un reato. Non utilizzate software che possa danneggiare la rete, creare problemi o allarmi di sicurezza, come port scanner, security scanner, network monitor, etc.

Segnalare tempestivamente qualsiasi variazione del comportamento della propria postazione di lavoro

È importante fare presenti tutti i problemi che si verificano perché possono essere il sintomo di un attacco in corso.

Segnalare comportamenti che possano far pensare a tentativi di ridurre la sicurezza del sistema informativo

Devono essere segnalate al Responsabile del Servizio Informatica, ad esempio, le richieste insistenti di altri utenti per avere accesso a postazioni di lavoro, dati o per conoscere password. Analogamente non devono essere presi in considerazione messaggi o telefonate che chiedono di compiere operazioni di cambio password o altre attività tecniche "poco chiare".

Utilizzo di supporto tecnico

Il personale può rivolgersi solo ai supporti tecnici "ufficiali" secondo le modalità indicate nei relativi contratti in essere e quindi non rivolgersi a personale di altre ditte o strutture oltre quelle previste. Il personale è tenuto a non comunicare alcuna informazione relativa a funzionalità e configurazioni della rete o delle postazioni di lavoro. Gli utenti devono controllare le configurazioni che i tecnici effettuano e, nel caso debba essere comunicata una password, questa deve essere cambiata subito dopo l'intervento. Deve essere segnalato qualsiasi dubbio, anche sull'operato del personale tecnico, al Responsabile del Servizio Informatica.

Non dare informazioni di alcun genere

Spesso, il vero hacker, non attacca il sistema per via informatica, ma utilizza tecniche di "ingegneria sociale", carpendo la fiducia dell'operatore che si trova ad essere il vero punto debole della catena di sicurezza. Non dare mai informazioni tecniche o organizzative di alcun genere, specialmente per telefono, anche a persone apparentemente conosciute. Un hacker utilizza tecniche molto sofisticate per ingannare il malcapitato, simulando situazioni che portano l'operatore a dargli fiducia.

27.4 Archivi cartacei temporanei

La gestione degli archivi cartacei temporanei si ascrive alla competenza del Responsabile del trattamento. Lo stesso individua le tipologie dei documenti contenenti i dati sensibili e giudiziari ed i dipendenti incaricati dei relativi trattamenti. Il Responsabile dovrà assicurare che la documentazione venga custodita in armadi dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato.

I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione dello stesso Responsabile o di un incaricato. Il Responsabile deve garantire l'integrità dei sottofascicoli in occasione dell'accesso all'archivio da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

Il Responsabile deve impedire l'accesso a persone prive di autorizzazione nei luoghi e nei momenti in cui si trattano dati sensibili e/o giudiziari.

Conseguentemente, il trattamento di dati sensibili e/o giudiziari contenuti in documenti cartacei deve avvenire per il tempo strettamente necessario, con successiva immediata archiviazione dei dati.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave. ,

Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure procedere all'identificazione su un apposito registro allo scopo predisposto.

27.5 Archivi cartacei di deposito

L'archivio cartaceo di deposito deve essere controllato, in considerazione della circostanza che l'accesso a tale documentazione non è pubblico.

Fermo restando quanto stabilito dall'Azienda con l'apposito "Regolamento per l'Archivio corrente, di deposito e storico", la consultazione degli archivi di deposito potrà avvenire esclusivamente da parte del personale autorizzato e da parte dei Responsabili degli archivi di ogni Struttura, per il materiale afferente la stessa.

I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sotto fascicoli in busta chiusa, con

sottoscrizione dello stesso Responsabile o di un incaricato della Struttura di riferimento della documentazione. Il Responsabile deve garantire l'integrità dei sotto fascicoli in occasione dell'accesso da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

27.6 Trattamenti con o senza l'ausilio di strumenti elettronici.

Il trattamento di dati senza strumenti elettronici riguarda i dati contenuti in tutti i supporti cartacei o simili, che comunque non richiedano l'uso di elaboratori elettronici. Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.

Per trattare i dati mediante dispositivi informatici, deve essere seguita una procedura di autenticazione che consenta l'identificazione del Responsabile o dell'Incaricato, mediante "credenziali di autenticazione". Le credenziali di autenticazione consistono in un user id, associato ad una parola chiave segreta (password). Le user id e Password individuali per l'accesso alle applicazioni non devono essere mai condivise con altri soggetti, anche se incaricati del trattamento. Nel caso in cui occorra permettere l'accesso da parte di altri utenti, è necessario richiedere la generazione di una nuova password.

Per ogni ulteriore disposizione ed istruzione in materia di Privacy finalizzata al corretto utilizzo di apparecchiature informatiche ed elettromedicali all'interno dell'Azienda, si rimanda alle Strutture competenti ed alle disposizioni di legge e regolamenti in materia.

27.6.1 - Custodia

I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili alle persone non incaricate del trattamento, mediante localizzazione presso spazi con accesso riservato (es. armadi o cassetti chiusi a chiave).

I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono essere ivi ricollocati al termine della giornata. I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

27.6.2 - Documenti contenenti dati sensibili e/o giudiziari

I documenti contenenti dati sensibili e/o giudiziari devono essere sottoposti al controllo dei Responsabili i quali, a loro volta, potranno avvalersi degli incaricati per la custodia e/o il trattamento.

27.6.3 - Gestione delle password

La password è assegnata ai Responsabili ed agli Incaricati mediante sistemi meccanici che consentano la generazione di password conformi alla normativa vigente. I Responsabili devono garantire l'esclusività dell'uso della password, in particolare impedendo che addetti al trattamento, o altri, si avvalgano di credenziali di autenticazione a qualunque titolo percepite. Nessuno deve annotare la propria password su supporti facilmente rintracciabili e, soprattutto, in prossimità della postazione di lavoro utilizzata.

I Responsabili devono altresì accertarsi che gli incaricati cambino la password almeno ogni sei mesi, ovvero se trattano dati sensibili e/o giudiziari ogni tre mesi.

ART. 28 – Violazione dei dati personali (*Data Breach*)

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.

Per questa ragione, anche sulla base della normativa europea, il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali *(data breach)* all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

L'ARNAS Garibaldi, rientra tra i soggetti previsti dal Regolamento Europeo cui incombe l'obbligo di comunicare entro 48 ore dalla conoscenza del fatto, con comunicazione tramite apposito modello tutte le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali contenuti nelle proprie banche dati. Pertanto è dovere di ogni dipendente di questa ARNAS segnalare al DPO tramite Mail all'indirizzo privacy@pec.ao-garibaldi.ct.it

ART. 29 – Applicazione ed entrata in vigore

Il presente Regolamento, adottato con deliberazione del Direttore Generale dell'Azienda, entra in vigore dalla data di esecutività della stessa, viene pubblicato nel sito Intranet aziendale, dandone contestuale comunicazione a tutto il personale dipendente al fine di consentirne la conoscenza e l'applicazione.

Il personale che dovesse trasgredire le regole presenti in ogni parte di questo documento, si assume la responsabilità per i danni eventualmente arrecati all'Azienda. I responsabili di tutte le UU.OO. sono tenuti a mettere in atto ogni misura di vigilanza e di controllo dell'attuazione delle disposizioni presenti in questo documento, affinché si osservino le regole descritte, allo scopo di evitare, oltre che l'applicazione delle sanzioni previste dalla normativa vigente, l'adozione delle correlate misure disciplinari. Si raccomanda a tutti la puntuale osservanza di quanto contenuto nel presente documento.

Allegati

- Atto di designazione - Responsabile esterno del trattamento dei dati personali
- Atto di designazione - Responsabile interno del trattamento dei dati personali
- Informativa ai sensi del regolamento UE 2016/679
- Contatti

ARNAS GARIBALDI CATANIA AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE

ATTO DI DESIGNAZIONE

Responsabile esterno del trattamento dei dati personali

Regolamento Unione Europea 2016/679

Con il presente documento, il Titolare del trattamento

VISTO: il Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio *(di seguito GDPR)* del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE *(regolamento generale sulla protezione dei dati)*

VISTO: Rettifica del Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 pubblicato sulla *Gazzetta ufficiale dell'Unione europea L 119 del 4 maggio 2016*

VISTO: Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU n.205 del 4-9-2018)

Vigente al: 19-9-2018

ATTESO

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare e/o dal Responsabile della Protezione dei Dati;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza e in particolare:
  - divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare e/o di altri Responsabili, ove nominati;
  - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  - la fase di raccolta del consenso dovrà essere preceduta dalla informativa e dal consenso degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione dovranno essere riservate.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

RITENUTO di provvedere a quanto sopra;

NOMINA

Il Dott. _____ nella qualifica di _____ della _____, *Responsabile esterno del trattamento dei dati personali* rilevati ai sensi Regolamento (UE) 2016/679 a cui spetta in generale il compito di garantire il pieno rispetto delle leggi in materia ed in particolare:

- individuare, formare e nominare gli incaricati del trattamento e successivamente diramare le istruzioni scritte necessarie per un corretto, lecito, sicuro trattamento;
- attuare gli obblighi di informazione e acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- vigilanza circa la corretta custodia e conservazione delle password e delle chiavi d'accesso agli armadi per la conservazione dei supporti magnetici o cartacei;
- controllo sulla effettiva adozione, da parte degli incaricati, di tutte le misure necessarie perché il trattamento dei dati personali avvenga nel pieno rispetto delle disposizioni di legge in materia e di quelle del Regolamento interno dell'ARNAS Garibaldi;
- vigilanza sul rispetto dei diritti di accesso degli interessati e con le modalità previste dalle norme di legge sopra richiamate;
- rispetto della sicurezza nel trattamento dei dati quanto alla custodia, alla cessazione e ai limiti di utilizzabilità, secondo quanto previsto dal Regolamento interno o dove non indicato dalla normativa vigente;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dal Regolamento (UE) 2016/679, in ordine, ove possibile, all'accesso ai dati e a tutti i diritti di aggiornamento, rettificazione, cancellazione e di opposizione;
- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni del Regolamento Aziendale sulla protezione dei dati, nonché adeguare il sistema alle norme regolamentari in materia di sicurezza, curandone l'applicazione da parte degli incaricati.
- Comunicare tempestivamente qualunque richiesta di accesso, accesso non autorizzato o eventuale anomalia di sicurezza del sistema al Responsabile della Protezione dei Dati Personali – Dott. Davide Morales.

Si precisa inoltre, che è facoltà del Titolare o del Responsabile della protezione dei Dati, procedere con verifiche periodiche al fine di garantire la reale applicazione di quanto sopra indicato.

Sottoscrivendo il presente atto, il dott._____

- conferma di conoscere gli obblighi assunti in relazione alle disposizioni del GDPR e di possedere i requisiti di esperienza, capacità ed affidabilità idonei richiesti;
- conferma di avere compreso integralmente le istruzioni qui impartite e si dichiarano competenti e disponibili alla piena esecuzione di quanto affidato;
- accetta la designazione a responsabile del trattamento dei dati personali e si impegna a rispettare le istruzioni ricevute.

*Catania, Data,*_____

Per conoscenza e accettazione

Dott. _____

ARNAS GARIBALDI CATANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE

ATTO DI DESIGNAZIONE

Responsabile interno del trattamento dei dati personali

Regolamento Unione Europea 2016/679

Con il presente documento, il Titolare del trattamento

VISTO: il Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio *(di seguito GDPR)* del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE *(regolamento generale sulla protezione dei dati)*

VISTO: Rettifica del Regolamento Europeo 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 pubblicato sulla *Gazzetta ufficiale dell'Unione europea L 119 del 4 maggio 2016*

VISTO: Decreto Legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU n.205 del 4-9-2018)

Vigente al: 19-9-2018

ATTESO

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare e/o dal Responsabile della Protezione dei Dati;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza e in particolare:
  - divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Titolare e/o di altri Responsabili, ove nominati;
  - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  - la fase di raccolta del consenso dovrà essere preceduta dalla informativa e dal consenso degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione dovranno essere riservate.

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

RITENUTO di provvedere a quanto sopra;

NOMINA

Il Dott. _____ nella qualifica di _____ dell'Unità Operativa Semplice/Complessa *Responsabile interno del trattamento dei dati personali* rilevati ai sensi Regolamento (UE) 2016/679 a cui spetta in generale il compito di garantire il pieno rispetto delle leggi in materia ed in particolare:

- catalogare analiticamente le banche dati e i sistemi installati con tutti gli elementi necessari, anche ai fini della eventuale notifica al Garante;
- individuare, formare e nominare gli incaricati del trattamento e successivamente diramare le istruzioni scritte necessarie per un corretto, lecito, sicuro trattamento;
- attuare gli obblighi di informazione e acquisizione del consenso, quando richiesto, nei confronti degli interessati;
- vigilanza circa la corretta custodia e conservazione delle password e delle chiavi d'accesso agli armadi per la conservazione dei supporti magnetici o cartacei;
- controllo sulla effettiva adozione, da parte degli incaricati, di tutte le misure necessarie perché il trattamento dei dati personali avvenga nel pieno rispetto delle disposizioni di legge in materia e di quelle del Regolamento interno dell'ARNAS Garibaldi;
- vigilanza sul rispetto dei diritti di accesso degli interessati e con le modalità previste dalle norme di legge sopra richiamate;
- rispetto della sicurezza nel trattamento dei dati quanto alla custodia, alla cessazione e ai limiti di utilizzabilità, secondo quanto previsto dal Regolamento interno o dove non indicato dalla normativa vigente;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dal Regolamento (UE) 2016/679, in ordine, ove possibile, all'accesso ai dati e a tutti i diritti di aggiornamento, rettificazione, cancellazione e di opposizione;
- collaborare per l'attuazione delle prescrizioni del Garante;
- predisporre ed aggiornare un sistema di sicurezza idoneo a rispettare le prescrizioni del Regolamento Aziendale sulla protezione dei dati, nonché adeguare il sistema alle norme regolamentari in materia di sicurezza, curandone l'applicazione da parte degli incaricati.
- Comunicare tempestivamente qualunque richiesta di accesso, accesso non autorizzato o eventuale anomalia di sicurezza del sistema al Responsabile della Protezione dei Dati Personali – Dott. Davide Morales.

Si precisa inoltre, che è facoltà del Titolare o del Responsabile della protezione dei Dati, procedere con verifiche periodiche al fine di garantire la reale applicazione di quanto sopra indicato.

Sottoscrivendo il presente atto, il dott._____

- conferma di conoscere gli obblighi assunti in relazione alle disposizioni del GDPR e di possedere i requisiti di esperienza, capacità ed affidabilità idonei richiesti;
- conferma di avere compreso integralmente le istruzioni qui impartite e si dichiarano competenti e disponibili alla piena esecuzione di quanto affidato;
- accetta la designazione a responsabile del trattamento dei dati personali e si impegna a rispettare le istruzioni ricevute.

*Catania, Data,*_____

Per conoscenza e accettazione

Dott. _____

ARNAS GARIBALDI CATANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE

Informativa ai sensi del regolamento UE 2016/679

Gentile Utente,

ai sensi del ***Regolamento Europeo*** *sul trattamento dei dati personali* ***nr. 679/2016****, La informiamo che il trattamento delle informazioni che La riguardano, sarà improntato ai principi di correttezza e liceità a tutela della Sua riservatezza e dei Suoi diritti in materia di privacy.*

Il rilascio delle informazioni contenute nel presente documento, unitamente alla manifestazione del relativo consenso debbono avvenire prima che il Titolare inizi il trattamento dei suoi dati. Tuttavia, esclusivamente nei casi previsti dal ***Regolamento Europeo*** *sul trattamento dei dati personali* ***nr. 679/2016,*** l'informativa potrebbe esserLe consegnata successivamente alle prestazioni effettuate dal Titolare. Questi casi sono:

- "impossibilità 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";
- "rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato".

Identità e dati di contatto del Titolare del trattamento:

Titolare del trattamento è il Direttore Generale dell'ARNAS Garibaldi, con sede legale a Catania, in Piazza Santa Maria di Gesù 5 - 95100. Codice fiscale e partita IVA 04721270876 .

Sarà possibile contattarci attraverso il numero telefonico 095.7591111 – 095.7595000 (il costo della chiamata dipende dal gestore telefonico del chiamante) oppure scrivendo al seguente indirizzo di posta elettronica ***privacy@pec.ao-garibaldi.ct.it***, anche per l'esercizio di tutti i diritti che Le sono riconosciuti dal Regolamento Europeo nr. 679/2016.

Identità e dati di contatto del Responsabile del Trattamento dei Dati:

L'ARNAS "Garibaldi" per consentire l'esercizio dei diritti previsti per interessato, secondo il Regolamento Europeo nr. 679/2016, *comunica che è suo diritto contattare il Responsabile per la protezione dei dati Dott. Davide Morales* scrivendo al seguente indirizzo di posta elettronica certificata ***privacy@pec.ao-garibaldi.ct.it.***

Modalità di raccolta e trattamento dei dati :

I dati possono essere raccolti tramite i software informatici in uso presso questa azienda o tramite moduli cartacei oppure Call Center Aziendale. Il trattamento avviene mediante strumenti automatizzati e cartacei nel rispetto della normativa. Il nostro sistema informatico è strutturato in modo da prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

a) Finalità del trattamento e conseguenze in caso di rifiuto.

1. *I dati personali da Lei forniti saranno trattati nel rispetto degli obblighi di riservatezza e della normativa vigente in materia di privacy. I Suoi dati saranno raccolti per le finalità previste dal trattamento e consentite dalla legge. La raccolta dei dati personali forniti (notizie anagrafiche, anamnestiche e documentazione clinica) o risultati di esami clinici, di laboratorio e strumentali, viene effettuata, dall'Azienda Ospedaliera Garibaldi, esclusivamente per finalità diagnostiche/ambulatoriali o di degenza ospedaliera sempre e comunque allo scopo di consentire la diagnosi e la cura del Suo stato di salute al fine di tutelare la Sua incolumità fisica. Potranno essere richiesti anche dati che riguardano familiari sia a fini anamnestici, sia per verificare la compatibilità, in alcuni casi, di patologie specifiche o di trattamenti sanitari particolari.*

2. *I trattamento dei dati è indispensabile per poter effettuare le prestazioni richieste e/o necessarie per la tutela della salute della persona assistita. Il mancato consenso al trattamento dei dati, con l'eccezione dei trattamenti in emergenza e di quelli disposti da Autorità Pubblica (Sindaco, Autorità Giudiziaria) comporta l'impossibilità di erogare la prestazione sanitaria.*

3. *I Suoi dati non saranno comunicati a terzi se non per i motivi consentiti dalla legge e per le finalità amministrative. In ogni caso, non saranno oggetto di diffusione. I dati potranno essere/saranno comunicati esclusivamente per i motivi connessi ai compiti istituzionali e per le finalità previste dal Regolamento Europeo nr. 679/2016. In particolare i sui dati verranno trattati esclusivamente all'interno dell'Azienda Ospedaliera Garibaldi, fatte salve le dovute comunicazioni:*
    - *all'ASP competente per esigenze gestionali e/o amministrative;*
    - *alla Regione Sicilia, ai fini contabili, di rimborso delle prestazioni offerte o di adempimento previsto espressamente dalla normativa vigente;*
    - *alla Compagnia Assicuratrice dell'Azienda in esecuzione della Polizza sottoscritta dall'Azienda;*
    - *all'Autorità Giudiziaria o di Polizia;*
    - *Ai soggetti pubblici o privati destinatari ai sensi di specifica normativa*

4. *La presente informativa ed il consenso da Lei prestato, anche in forma orale, si riferiscono alla pluralità delle prestazioni erogate, anche in tempi diversi, dalle Unità operative complesse che Le forniscono assistenza in ospedale durante e dopo la degenza.*

5. *Il Titolare del trattamento è il Direttore Generale dell'Azienda Ospedaliera di Rilievo Nazionale Garibaldi.*

6. *I Direttori delle Strutture Complesse ed i Responsabili delle Strutture Semplici afferenti ai Dipartimenti sanitari ed allo Staff della Direzione Sanitaria sono responsabili dei trattamenti dei dati effettuati nelle rispettive strutture, mentre il Direttore Sanitario è responsabile del trattamento di conservazione delle cartelle cliniche dal momento della loro consegna all'Archivio centrale cartelle cliniche. Presso l'U.R.P. e gli uffici di accettazione amministrativa delegati, l'interessato potrà esercitare i propri diritti ai sensi dell'art.8 della citata legge; presso tali uffici sono inoltre disponibili le informazioni relative agli altri Responsabili per il trattamento dati. L'elenco aggiornato dei responsabili è disponibile inoltre sul sito dell'Ente, all'indirizzo http://www.ao-garibaldi.ct.it*

Diritti dell'interessato

In ogni momento l'interessato potrà esercitare i Suoi diritti nei confronti del Titolare del trattamento, quali:

- *esercitare l'opposizione al trattamento in tutto o in parte;*
- *ottenere la cancellazione dei dati in possesso del titolare;*
- *ottenere l'aggiornamento o la rettifica dei dati conferiti;*
- *chiedere ed ottenere in forma intellegibile i dati in possesso del titolare (diritto di accesso);*
- *chiedere ed ottenere trasformazione in forma anonima dei dati;*
- *chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento.*

Inoltre, l'informativa e il consenso al trattamento dei dati personali possono intervenire, senza ritardo, successivamente alla prestazione, anche nel caso in cui la prestazione medica può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia.

Contatti:

Titolare del Trattamento:

- *Azienda Ospedaliera di Rilievo Nazionale e di Alta Specializzazione Garibaldi*

  Piazza Santa Maria del Gesù, 5 – 95123 Catania

  Telefono: 095.7593856

Responsabile della Protezione dei Dati:

- *Dott. Davide Morales – E-Mail privacy@pec.ao-garibaldi.ct.it*

  Piazza Santa Maria del Gesù, 5 – 95123 Catania

  Telefono: 095.7593667 - 335.7476244

Garante per la protezione dei dati personali:

- *www.GarantePrivacy.it*