COPIA

AZIENDA U.S.L.

PESCARA

Il giorno 30 GIU. 2009 nella sede dell'Unità Sanitaria Locale di Pescara.

IL DIRETTORE GENERALE

Dott. Claudio D'Amario, nominato dalla Giunta Regionale con deliberazione n. 50 del 14 febbraio 2009, acquisiti i pareri allegati del Direttore Amministrativo e del Direttore Sanitario, ha adottato il seguente provvedimento, su proposta dell'Ufficio aziendale Privacy:

N. 436

OGGETTO:

OGGETTO: MISURE ED ACCORGIMENTI PRESCRITTI AI TITOLARI DEI TRATTAMENTI EFFETTUATI CON STRUMENTI ELETTRONICI RELATIVAMENTE ALLE ATTRIBUZIONI DELLE FUNZIONI DI AMMINISTRATORE. DI SISTEMA *GIUSTO PROVVEDIMENTO* GARANTE *PROTEZIONE DATI PERSONALI DEL 27/11/2008)*

IL DIRETTORE GENERALE

Letta la relazione, riportata nell'Allegato A, del Referente Aziendale Privacy e dell'Amministratore di Sistema, vista la proposta a firma del Direttore Dipartimento. Economico Finanziario/A.B.S./Ufficio. Informatica, Statistica e CED e ritenuto di condividere quanto in essa contenuto;

- Acquisiti i pareri del Direttore Sanitario e del Direttore Amministrativo riportati nell'Allegato B;

Ravvisata la necessità di conferire al presente provvedimento effetti di immediata esecutività stante l'urgenza del provvedere;

DELIBERA

1. di formalizzare le seguenti Piattaforme Informatiche Aziendali :

- **Piattaforma Ospedaliera** (Gestione Reparti; CUP, Pronto Soccorso ed Accettazione;Cartelle cliniche, ADI e Riabilitazione);
- **Piattaforma Diagnostica** (Laboratorio Analisi, Trasfusionale, Radiologia, Medicina Nucleare, Sw di Screening);
- **Piattaforma Economica-finanziaria**;
- **Piattaforma Gestionale-Risorse Umane;**
- **Piattaforma SW Aziendali/Regionali/Nazionali**;
- **Piattaforma SW Applicativi aziendali** (Sogei,-Tessera Sanitaria, Scelta e revoca, rapporti ASL-MMG-Medici convenzionati e/o specialisti)

2. di stabilire che il Sistema Informativo Aziendale (d'ora in avanti, S.I.A.) risulta composto ed integrato su **3 macro aree**:

- **Infrastruttura Hardware** di cui fa parte l'intera Server Farm, la SAN, lo Storage pool per il backup dati, tutti gli altri server che governano determinati servizi/applicativi ASL e per finire l'intero parco delle postazioni informatiche che sono utilizzate nei vari Servizi e/o Dipartimenti;
- **Infrastruttura di Comunicazione**: ci si riferisce all'insieme degli apparati di rete e delle linee dati che permettono la comunicazione di tutto il S.I.A. articolato su tutta la dislocazione geografica della ASL (base provinciale);

a. **Infrastruttura Software:** si racchiudono in essa tutte le piattaforme sw che sono implementate nella ASL partendo dall'area ospedaliera in tutte le sue direttrici principali e secondarie fino ad arrivare agli applicativi che afferiscono alle comunicazioni con altre strutture regionali e/o nazionali (es: Sogei-Tessera Sanitaria, Scelta e Revoca dei MMG. ecc.)

3 di stabilire che la nomina degli Amministratori di Sistema (A.d.S.), e dei Referenti aziendali di .Piattaforma (R.A.P.)., così come la redazione di un "Regolamento di gestione utenti e profili di autorizzazione per trattamenti elettronici" vengano fatte dal Titolare del trattamento con successivo atto deliberativo;

4. di individuare i seguenti compiti che l'Amministratore di Sistema. dovrà adempiere:
   - assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda;

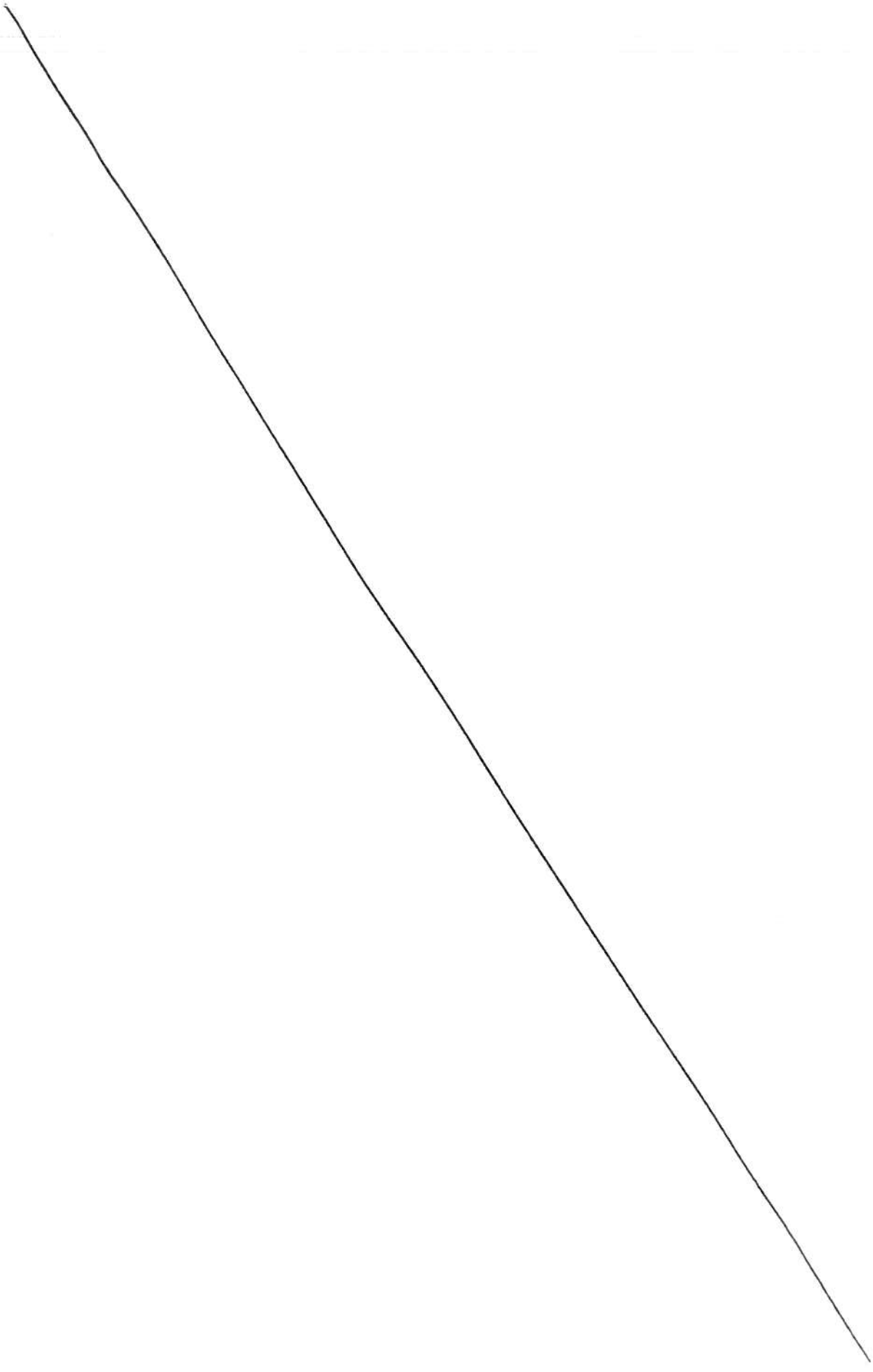
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di Backup e Disaster recovery) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; dette registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- vigilare sull'attività dei preposti;
- attribuire a ciascun utente o incaricato del trattamento un codice identificativo personale per l'utilizzazione dell'elaboratore;
- assegnare e gestire i codici identificativi personali in modo che possano essere disattivati in caso di loro perdita;
- adottare idonee misure di protezione dei dati inseriti all'interno degli elaboratori o accessibili attraverso l'utilizzo di altri elaboratori;
- assistere il titolare (e l'eventuale responsabile) nella gestione dei supporti e delle aree di memoria;
- assistere il titolare (e l'eventuale responsabile) nella conservazione e custodia dei supporti.

5 di individuare i seguenti compiti che il Referente Aziendale di Piattaforma dovrà adempiere:

- è l'interfaccia unica, per la piattaforma di competenza, con l'A.d.S. per quanto attiene alla gestione degli incaricati (credenziali di autenticazione e profili di autorizzazione);
- aggiorna annualmente, comunicandole al Direttore Generale per il tramite dell'Ufficio Privacy entro il mese di febbraio:
  - la scheda riepilogativa della piattaforma informatica di competenza,
  - le strutture organizzative coinvolte nell'utilizzo della piattaforma,
  - i profili standard di autorizzazione (di concerto con l'A.d.S.);
  - per le unità organizzative coinvolte nell'utilizzo della piattaforma redige il modulo di indicazione degli incaricati e dei relativi profili di autorizzazione;
  - si relaziona con le unità organizzative coinvolte nell'uso della piattaforma:
  - raccoglie, dalle strutture organizzative coinvolte, l'indicazione (di competenza dei Responsabili del trattamento) delle persone incaricate di trattamento elettronico e dei relativi profili di autorizzazione,
  - revisiona e consolida tali indicazioni chiedendo, se opportuno, integrazioni e precisazioni,
  - comunica tali indicazioni all' A.d.S.,
  - cura l'archiviazione di tali comunicazioni;
  - verifica annualmente, entro il mese di febbraio, con la supervisione dell'A.d.S., la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

6 di notificare il presente atto a tutti i soggetti nominati Responsabili del trattamento dei dati personali, al Responsabile del Servizio Informativo Aziendale (S.I.A) ed agli Uffici e Servizi della ASL interessati.

7. Di dichiarare il presente atto immediatamente esecutivo.



AU. A

RELAZIONE DEL REFERENTE AZIENDALE PRIVACY E DELL'AMMINISTRATORE DI SISTEMA

Visto il Provvedimento del Garante per la Protezione dei Dati Personali adottato il 27 novembre 2008 e recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

Considerato che attraverso il citato Provvedimento l'Autorità ha stabilito una serie di obblighi a carico del Titolare del trattamento dei dati personali;

Nello specifico la novità più rilevante contenuta nel Provvedimento, di cui all'oggetto è che sono stati individuati con il termine di "amministratore di sistema" le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e che sono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati. Per cui sono stati ricondotti a tale professione anche coloro "*che svolgono mansioni analoghe in rapporto a sistemi di elaborazione e banche di dati*". Ci si riferisce:
a) all'amministratore di sistemi software complessi,
b) all'amministratore di apparati di sicurezza,
c) all'amministratore di basi di dati,
d) all'amministratore di rete,
e) all'amministratore di sistema;

Atteso che il termine per gli adempimenti è fissato al prossimo 30 giugno c.a.,

Considerato che:

la figura **dell'Amministratore di sistema** (d'ora in avanti, **A.d. S.**) fu introdotta con Decreto del Presidente della Repubblica n. 318/1999, non più in vigore, che lo definiva come "*il soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione.*";

la Azienda USL di Pescara (d'ora in avanti, ASL) nominò detta figura con atto deliberativo n. 423 dell'8 aprile 2003, la stessa non è stata mai eliminata, anzi è stata confermata nel corso degli anni tant'è che oggi opera nella figura del Dott. Domenico Trotta, giusta Delibera n. 1594 del 1° dicembre 2004.

Attesa la rilevanza che tali figure rivestono nel trattamento dei dati personali in modalità informatica, in particolare alla luce degli obblighi relativi all'applicazione delle misure di sicurezza, l'Autorità per la protezione dei dati personali ha disposto quanto segue:

1. i titolari del trattamento, devono "*valutare con particolare attenzione l'attribuzione di funzioni tecniche propriamente corrispondenti o assimilabili a quelle di amministratore di sistema, amministratore (system administrator) di base di dati (database administrator) o amministratore di rete (network administrator), laddove tali funzioni siano esercitate in un contesto che renda ad essi tecnicamente possibile l'accesso, anche fortuito, a dati personali.*"
2. in merito alla nomina dell' A.d.S., tale figura professionale si dedica alla gestione ed alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati ed i sistemi software complessi

utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;

3. la nomina degli A.d.S. va fatta previa valutazione delle caratteristiche soggettive, relativamente alla "*esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso, il profilo relativo alla sicurezza*";
4. l'A.d.S. ha il compito di: realizzare copie di sicurezza (operazioni di backup e disaster recovery dei dati); custodire le credenziali alla gestione dei sistemi di autenticazione e di autorizzazione;
5. l' A.d.S. va designato individualmente, utilizzando nome, cognome, funzione o area organizzativa di appartenenza; assicurando una elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
6. va presa in considerazione la possibilità di effettuare nomine plurime di A.d.S., specificando "*l'elenco delle funzioni ad essi attribuite*". La designazione, singola o plurima, va riportata nel Documento Programmatico sulla Sicurezza (d'ora in avanti, DPS).
7. nell'ipotesi in cui l'attività del/degli A.d.S. "*riguardi anche indirettamente servizi o sistemi che trattano o permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari...sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni...*". La comunicazione potrà avvenire ricorrendo ad una delle seguenti modalità: "*avvalendosi dell'informativa resa agli interessati...nell'ambito del rapporto di lavoro che li lega al titolare oppure...mediante altri strumenti di comunicazione interna...*";
8. nel caso, poi, di servizi di amministrazione di sistema affidati in outsourcing il titolare avrà l'obbligo conservare gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;
9. va calendarizzata una attività di verifica nei confronti dell'A.d.S., da svolgersi almeno a cadenza annuale; al fine di controllare la rispondenza o meno alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalla normativa vigente;
10. necessita predisporre un sistema di "*registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.*" Gli *access log* devono avere le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; pertanto le registrazioni devono avere i riferimenti temporali certi e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo (non inferiore a sei mesi).

Considerato che il Sistema Informativo aziendale (d'ora in avanti, S.I.A.) risulta così composto ed integrato su **3 macro aree**:

- **Infrastruttura Hardware** di cui fa parte l'intera Server Farm, la SAN, lo Storage pool per il backup dati, tutti gli altri server che governano determinati servizi/applicativi ASL e per finire l'intero parco delle postazioni informatiche che sono utilizzate nei vari Servizi e/o Dipartimenti;
- **Infrastruttura di Comunicazione**: ci si riferisce all'insieme degli apparati di rete e delle linee dati che permettono la comunicazione di tutto il S.I.A. articolato su tutta la dislocazione geografica della ASL (base provinciale);

- **Infrastruttura Software:** si racchiudono in essa tutte le piattaforme sw che sono implementate nella ASL partendo dall'area ospedaliera in tutte le sue direttrici principali e secondarie fino ad arrivare agli applicativi che afferiscono alle comunicazioni con altre strutture regionali e/o nazionali (es: Sogei-Tessera Sanitaria, Scelta e Revoca dei MMG, ecc.).

Considerato che gli ambiti di operatività dell'AdS e dei Referenti Aziendali di Piattaforma (d'ora in avanti, RAP) possono essere rappresentati sulle seguenti piattaforme hardware/software:

- Piattaforma Aix/Linux/Unix/Solaris;
- Piattaforma Windows/VmWare;
- Piattaforma Networking;
- Piattaforma di database Oracle –DBA Oracle;
- Piattaforma di database RDBMS;
- Piattaforma di Referenti Applicativi

A tal proposito si esplicitano i ruoli e/o competenze delle piattaforme hardware/software evidenziate:

- **Piattaforma UNIX/Solaris/Linux**

Gli Amministratori di Sistema con profilo di autorizzazione di amministratore di piattaforma UNIX / Solaris sono autorizzati ad operare su tutti i sistemi della piattaforma UNIX/

- **Piattaforma Windows/VmWare**

Gli Amministratori di Sistema con profilo di autorizzazione di amministratore di piattaforma Windows/VmWare sono autorizzati ad operare su tutti i sistemi della piattaforma Windows/VmWare

- **Piattaforma Networking**

Gli Amministratori di Sistema con profilo di autorizzazione di amministratore di rete sono autorizzati ad operare su tutti i sistemi di rete compresi i sistemi di servizio (Radius, DHCP, DNS, VPN Server, WCS, ecc.

- **Piattaforma di database Oracle – DBA Oracle**

Gli Amministratori di Sistema con profilo di autorizzazione di amministratore di database sono autorizzati ad operare su tutti i sistemi database Oracle

- **Piattaforma di database RDBMS**

Gli Amministratori di Sistema con profilo di autorizzazione di sistemista amministratore di RDBMS sono autorizzati ad operare sui sistemi RDBMS non standard per APSS (diversi da Oracle) come ad esempio (MS SQL Server, MySQL, Informix, ecc) utilizzati da trattamenti di dati aziendali

- **Piattaforma di Referenti Applicativi**

Gli Amministratori di Sistema con profilo di autorizzazione di Referente Applicativo sono autorizzati ad operare sui sistemi utilizzati dal trattamento di cui sono referenti applicativi

Poiché le professionalità attualmente in servizio presso il CED dell'Azienda sono le seguenti:

- Ferrara Isidoro (liv. B0);
- Rasetti Giacinto(liv C1);
- Pece Alessandro(liv. D0)
- Trotta Domenico (liv. D1)

Considerato che sono state censite ed individuate le seguenti **Piattaforme Informatiche Aziendali (P.I.A.)** :

- **Piattaforma Ospedaliera** (Gestione Reparti; CUP, Pronto Soccorso ed Accettazione;Cartelle cliniche, ADI e Riabilitazione);

- **Piattaforma Diagnostica** (Laboratorio Analisi, Trasfusionale, Radiologia, Medicina Nucleare, Sw di Screening);
- **Piattaforma Economica-finanziaria;**
- **Piattaforma Gestionale-Risorse Umane;**
- **Piattaforma SW Aziendali/Regionali/Nazionali;**
- **Piattaforma SW Applicativi aziendali** (Sogei,-Tessera Sanitaria, Scelta e revoca, rapporti ASL-MMG-Medici convenzionati e/o specialisti)

Ravvisato,quindi, che allo stato attuale non è possibile provvedere alla copertura delle singole Piattaforme informatiche assegnando alle stesse una singola unità nominata R.A.P., ma si dovrà procedere, al fine di dare attuazione al sopra citato Provvedimento del Garante, a nomine che prevedano l'attribuzione ad un singolo A.d.S. / R.A.P. di più Piattaforme informatiche;

Propone

1. di formalizzare le seguenti **Piattaforme Informatiche Aziendali** (d'ora in avanti, **P.I.A.**) :
- **Piattaforma Ospedaliera** (Gestione Reparti; CUP, Pronto Soccorso ed Accettazione;Cartelle cliniche, ADI e Riabilitazione);
- **Piattaforma Diagnostica** (Laboratorio Analisi, Trasfusionale, Radiologia, Medicina Nucleare, Sw di Screening);
- **Piattaforma Economica-finanziaria;**
- **Piattaforma Gestionale-Risorse Umane;**
- **Piattaforma SW Aziendali/Regionali/Nazionali;**
- **Piattaforma SW Applicativi aziendali** (Sogei,-Tessera Sanitaria, Scelta e revoca, rapporti ASL-MMG-Medici convenzionati e/o specialisti)

2. di stabilire che il Sistema Informativo Aziendale (d'ora in avanti, S.I.A.) risulta composto ed integrato su **3 macro aree**:

- **Infrastruttura Hardware** di cui fa parte l'intera Server Farm, la SAN, lo Storage pool per il backup dati, tutti gli altri server che governano determinati servizi/applicativi ASL e per finire l'intero parco delle postazioni informatiche che sono utilizzate nei vari Servizi e/o Dipartimenti;
- **Infrastruttura di Comunicazione**: ci si riferisce all'insieme degli apparati di rete e delle linee dati che permettono la comunicazione di tutto il S.I.A. articolato su tutta la dislocazione geografica della ASL (base provinciale);
- **Infrastruttura Software:** si racchiudono in essa tutte le piattaforme sw che sono implementate nella ASL partendo dall'area ospedaliera in tutte le sue direttrici principali e secondarie fino ad arrivare agli applicativi che afferiscono alle comunicazioni con altre strutture regionali e/o nazionali (es: Sogei-Tessera Sanitaria, Scelta e Revoca dei MMG, ecc.)

3. di stabilire che la nomina degli A.d.S. e degli R.A.P.., così come la redazione di un "Regolamento di gestione utenti e profili di autorizzazione per trattamenti elettronici" vengano fatte dal Titolare del trattamento con successivo atto deliberativo;

4. di individuare i seguenti compiti che l'Amministratore di Sistema (A.d.S.) dovrà adempiere:

- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso presso la ASL;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di Backup e Disaster recovery) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici; dette registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
- vigilare sull'attività dei preposti;
- attribuire a ciascun utente o incaricato del trattamento un codice identificativo personale per l'utilizzazione dell'elaboratore;
- assegnare e gestire i codici identificativi personali in modo che possano essere disattivati in caso di loro perdita;
- adottare idonee misure di protezione dei dati inseriti all'interno degli elaboratori o accessibili attraverso l'utilizzo di altri elaboratori;
- assistere il titolare (e l'eventuale responsabile/i) nella gestione dei supporti e delle aree di memoria;
- assistere il titolare (e l'eventuale responsabile/i) nella conservazione e custodia dei supporti.
- definisce, per le unità organizzative coinvolte nell'utilizzo della piattaforma, il modulo di indicazione degli incaricati e dei relativi profili di autorizzazione;
- tiene i rapporti con le unità organizzative coinvolte nell'uso della piattaforma:

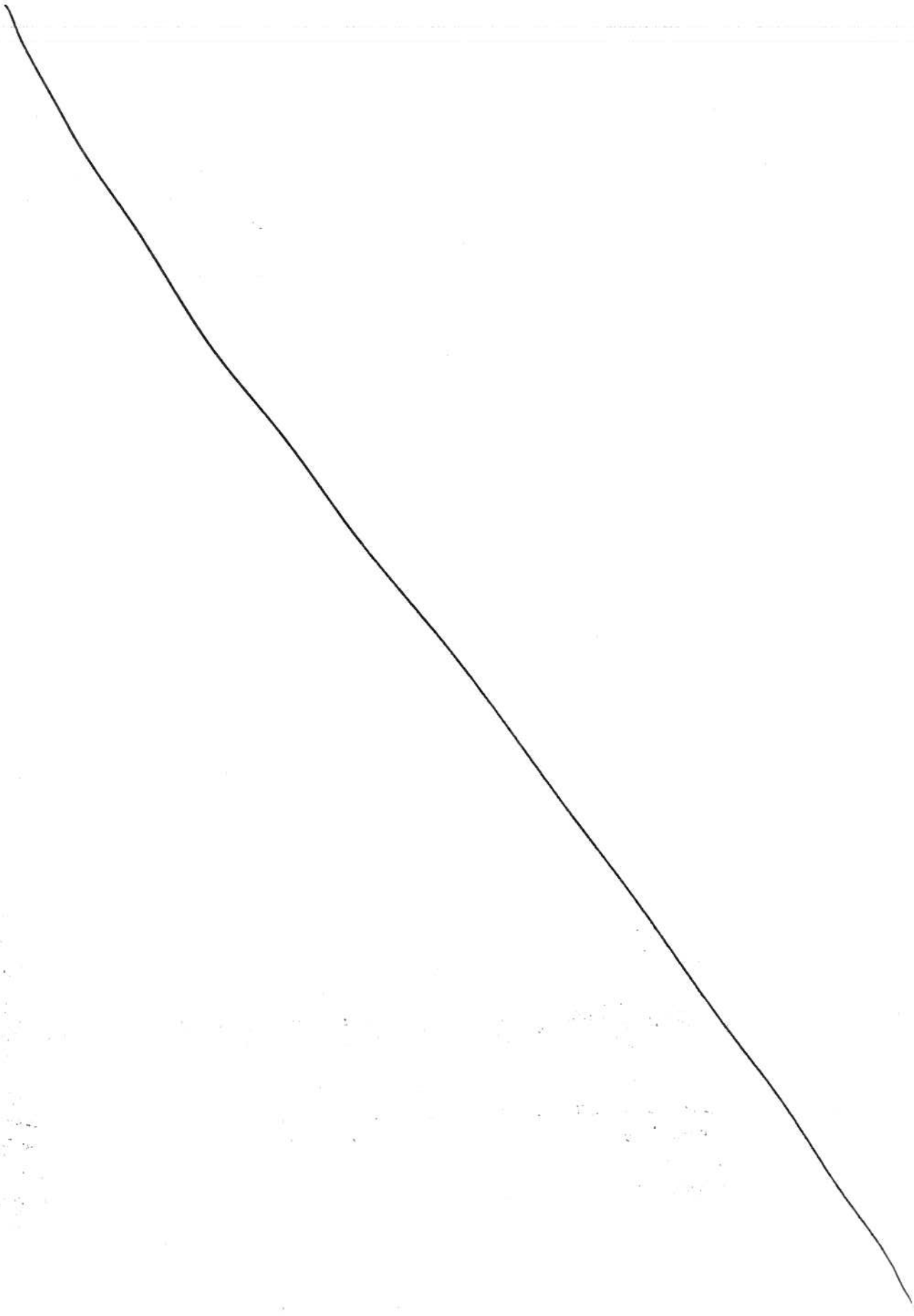
5. di individuare i seguenti compiti che il Referente Aziendale di Piattaforma deve adempiere:

- è l'interfaccia unica, per la piattaforma di competenza, con l'A.d.S. per quanto attiene alla gestione degli incaricati (credenziali di autenticazione e profili di autorizzazione);
- aggiorna annualmente, comunicandole al Direttore Generale per il tramite dell'Ufficio Privacy entro il mese di febbraio:
  - la scheda riepilogativa della piattaforma informatica di competenza,
  - le strutture organizzative coinvolte nell'utilizzo della piattaforma,
  - i profili standard di autorizzazione (di concerto con l'A.d.S.);
  - per le unità organizzative coinvolte nell'utilizzo della piattaforma redige il modulo di indicazione degli incaricati e dei relativi profili di autorizzazione;
  - si relaziona con le unità organizzative coinvolte nell'uso della piattaforma:
  - raccoglie, dalle strutture organizzative coinvolte, l'indicazione (di competenza dei Responsabili del trattamento) delle persone incaricate di trattamento elettronico e dei relativi profili di autorizzazione,
  - revisiona e consolida tali indicazioni chiedendo, se opportuno, integrazioni e precisazioni,
  - comunica tali indicazioni all' A.d.S.,
  - cura l'archiviazione di tali comunicazioni;
  - verifica annualmente, entro il mese di febbraio, con la supervisione dell'A.d.S., la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

6 di notificare il presente atto a tutti i soggetti nominati Responsabili del trattamento dei dati personali, al Responsabile del Servizio Informativo Aziendale (S.I.A) ed agli Uffici e Servizi della ASL interessati.

AMMINISTRATORE DI SISTEMA
F.to Dott. Domenico Trotta

REFERENTE AZ.LE PRIVACY
F.to Dott. Giovanni Modesti



Allegato B - Copia -

Si attesta la regolarità tecnica ed amministrativa, nonché la legittimità del provvedimento in questione.

IL DIRETTORE DIP. ECONOMICO FINANZIARIO/A.B.S./UFF. INFORMATICA, STATISTICA E CED
F.to (Dott.ssa Maria Ruffini)

Si attesta, che la spesa risulta imputata sulla voce di conto n. _____ del Bilancio che presenta sufficiente disponibilità.

IL DIRETTORE DIP. ECONOMICO FINANZIARIO/A.B.S./UFF. INFORMATICA, STATISTICA E CED
F.to (Dott.ssa Maria Ruffini)

Ai sensi del D. Lgs. 502/92 e successive modificazioni ed integrazioni, il sottoscritto esprime il seguente parere sul presente provvedimento:

IL DIRETTORE AMMINISTRATIVO
F.to (Dott. ssa Tea Di Pietro)

IL DIRETTORE SANITARIO
F.to (Dott. Fernando Guarino)

IL DIRETTORE GENERALE

F.to Dott. Claudio D'Amario

Pubblicato all'albo dell'ente per 15 giorni dal - 3 LUG. 2009 al 17 LUG. 2009

inviata per l'esecuzione

a: Gest. Econ. Finanz. UFF. A2. PRIVACY

per conoscenza a: CED

inviata alla Giunta Regionale in data _____ prot. n. _____

inviata al Presidente Conferenza dei Sindaci in data _____ prot. n. _____

inviata al Collegio Sindacale in data _____ prot. n: _____

Per copia conforme all'originale

- 3 LUG. 2009

IL FUNZIONARIO

SETTORE AA.GG.