Sistema Sanitario Regionale Piemonte
Azienda Ospedaliera Nazionale
SS. ANTONIO e BIAGIO
e CESARE ARRIGO
Alessandria

Sede legale: via Venezia n.16 - 15100 Alessandria. Codice fiscale/Partita IVA: 01640560064.
Telefono: (0131) 206111. Telefax: (0131) 236227

VERBALE DI DELIBERAZIONE DEL DIRETTORE GENERALE

DELIBERAZIONE N° 77

L'anno duemilaquattordici il giorno quattro del mese di marzo in una sala degli Uffici Amministrativi dell'Azienda Ospedaliera "SS. Antonio e Biagio e C. Arrigo" - via Venezia, 16 - 15100 Alessandria

IL DIRETTORE GENERALE

DOTT.NICOLA GIORGIONE

ai sensi della D.G.R. n.18 - 3728 del 27.4.2012

Acquisito il parere del - DIRETTORE AMMINISTRATIVO - dott. Francesco ARENA
- DIRETTORE SANITARIO - dott. Luciano BERNINI

adotta la deliberazione all'oggetto indicato:

DOCUMENTO AZIENDALE SULLA SICUREZZA IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL D.LGS. 30 GIUGNO 2003 N.196. APPENDICE DI AGGIORNAMENTO ANNO 2014

Mod. AA.GG. e RP 02 - 05

DELIBERAZIONE N. 77 DEL - 4 MAR. 2014

OGGETTO: DOCUMENTO AZIENDALE SULLA SICUREZZA IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI AI SENSI DEL D.LGS. 30 GIUGNO 2003 N.196. APPENDICE DI AGGIORNAMENTO ANNO 2014.

IL DIRETTORE GENERALE

Su proposta n. 73 del 20/02/2014 della S.S.A. Legale dalla cui istruttoria si evince che:

PREMESSO che con Decreto Legislativo 30 giugno 2003 n.196 è stato approvato il "Codice in materia di protezione dei dati personali", entrato in vigore con decorrenza 1 gennaio 2004;

RICHIAMATO l'art.31 del Codice che pone a carico dei soggetti che trattano dati personali, l'obbligo di adottare idonee e preventive misure di sicurezza, in modo da eliminare o ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

RICHIAMATO altresì l'art.33 del Codice che obbliga i titolari del trattamento ad adottare comunque misure di sicurezza, volte ad assicurare un livello minimo di protezione dei dati personali

RILEVATO che l'art. 45 del D.L. n.5/2012 ha espressamente abrogato l'obbligo dell'art.34 comma 1 lett. g) del Codice che prevedeva la tenuta di un aggiornato Documento Programmatico sulla Sicurezza, da redigersi a cura del Titolare entro il 31 marzo di ciascun anno, con i contenuti indicati dal punto 19 del Disciplinare Tecnico riportato nell'Allegato B al D.Lgs.196/2003;

DATO ATTO che per un continuo monitoraggio delle misure aziendali adottate in materia di trattamento di dati personali è stato in ogni caso richiesto alla S.C. Sistemi informativi e Logistici e CDG di comunicare le variazioni intervenute all'architettura del sistema informativo aziendale e alla S.C. Acquisti e Gestione servizi Economali di indicare le modificazioni alla gestione esterna di servizi strumentali aziendali interessati al trattamento dei dati personali dell'utenza come riassunte nell'appendice allegata;

PRESO ATTO che in ragione delle variazioni intervenute nell'avvicendamento dei Responsabili di numerose Strutture Sanitarie aziendali è stato conseguentemente aggiornato altresì l'elenco dei nominativi dei Responsabili del Trattamento dei dati personali;

VALUTATA l'idoneità delle restanti misure aziendali di sicurezza adottate nel trattamento di dati personali descritte nel documento approvato con deliberazione n.59 del 27/02/2013 e l'opportunità di provvedere all'aggiornamento delle stesse nel momento in cui l'operatività del nuovo Atto Aziendale andrà a modificare la tipologia dei dati trattati da ciascuna Struttura;

ASSUNTA la correttezza del processo istruttorio correlato, la cui responsabilità è riconducibile all'ambito dirigenziale;

RITENUTO di condividere la sopra richiamata proposta;

ACQUISITO il parere obbligatorio e favorevole del Direttore Sanitario nonché quello favorevole del Direttore Amministrativo, ciascuno per quanto di competenza,

DELIBERA

di approvare l'Appendice di variazione al vigente Documento Aziendale sulla Sicurezza in materia di misure minime di sicurezza in materia di Privacy, allegata alla presente deliberazione quale parte sostanziale ed integrante;

di notificare a cura della SSA Legale, il presente provvedimento, a tutti i Responsabili del trattamento, come individuati e nominati con il presente provvedimento, che ne cureranno la diffusione e l'osservanza da parte degli Incaricati dei trattamenti appartenenti alle rispettive strutture.

IL DIRETTORE GENERALE
Dr. Nicola GIORGIONE

APPENDICE
al Documento Aziendale sulla Sicurezza adottato dall'Azienda Ospedaliera Nazionale di Alessandria in osservanza al Decreto Legislativo 30 giugno 2003 n.196.

INDICE

1. Introduzione e Scopo del Lavoro

Con l'entrata in vigore del Decreto Legislativo 30 giugno 2003 n.196, "Codice in materia di protezione dei dati personali", avvenuta con decorrenza 1 gennaio 2004, è stata disposta la contestuale abrogazione di tutte le disposizioni elencate all'art.183 del predetto provvedimento, tra cui la Legge n.675/1996, il D.Lgs. n.135/1999 il D.Lgs. n.282/1999 ed il D.P.R. n.318/1999.
Tuttavia, l'obbligo di adozione di misure minime di sicurezza è stato ribadito dagli artt.31-36 del Codice.
In particolare, l'art. 34 comma 1 lett. g) prevedeva la tenuta di un aggiornato Documento Programmatico sulla Sicurezza, da redigersi a cura del Titolare entro il 31 marzo di ciascun anno, con i contenuti indicati dal punto 19 del Disciplinare Tecnico riportato nell'Allegato B al D.Lgs.196/2003;
L'art. 45 del D.L.n.5/2012 conv.dalla L. n.35/2012 ha espressamente abrogato il suddetto obbligo; tuttavia l'Azienda ritiene opportuno adottare un documento aziendale da aggiornare con cadenza annuale che monitori le misure di sicurezza aziendali adottate in materia di trattamento dei dati personali.
Con deliberazione n.59 del 27/02/2013 è stato Adottato il documento Aziendale per la sicurezza aggiornato al 2013.
Con la presente appendice per un continuo monitoraggio delle misure aziendali adottate in materia di trattamento di dati personali si procede all'aggiornamento delle variazioni intervenute all'architettura del sistema informativo aziendale e delle modificazioni alla gestione esterna di servizi strumentali aziendali interessati al trattamento dei dati personali dell'utenza

Inoltre, in ragione delle variazioni intervenute nell'avvicendamento dei Responsabili di numerose Strutture Sanitarie aziendali si aggiorna conseguentemente l'elenco dei nominativi dei Responsabili del Trattamento dei dati personali;

Le restanti misure aziendali di sicurezza adottate nel trattamento di dati personali descritte nel documento approvato con deliberazione suddetta a cui si rinvia per i punti non richiamati nella presente appendice sono tuttora operative e idonee a garantire il rispetto della vigente normativa.

2 Distribuzione dei compiti e delle responsabilità

2.1.1. Il Titolare del trattamento

Ai sensi dell'art. 4 comma 1 lett. f) del Codice, il Titolare del trattamento è l'Azienda Ospedaliera "SS.Antonio e Biagio e Cesare Arrigo" con sede legale in Alessandria, Via Venezia 16, in persona del suo legale rappresentante pro tempore.
Il Titolare del trattamento:

- approva il Documento Aziendale per la Sicurezza
- nomina i Responsabili del trattamento
- individua la figura dell'Amministratore del Sistema
- adotta tutti i provvedimenti di carattere generale concernenti il rispetto della normativa sulla privacy ed in particolar modo quelli attinenti all'adozione delle misure di sicurezza

2.1.2 I Responsabili del trattamento

La nomina dei Responsabili del Trattamento è stato effettuato in base ad un criterio che tenesse conto delle specifiche competenze e dell'esperienza necessarie ad assicurare idonea garanzia del rispetto della normativa ed in particolare del rispetto delle misure di sicurezza adottate dal Titolare.
Con la nota prot.n.2430/DG del 20.7.1998, i Responsabili/Referenti di Strutture Operative, ciascuno per le attività svolte e per il trattamento dei dati di rispettiva pertinenza, sono stati nominati "Responsabili del trattamento", con i compiti di cui ora all'art.29 del Codice.
Alla luce delle modifiche apportate all'organizzazione aziendale a seguito dell'adozione del nuovo Atto aziendale, i "Responsabili del trattamento" sono individuati nei Responsabili/Referenti di tutte le Strutture Complesse (S.C.) e Semplici a valenza Dipartimentale (SSD), o aziendale (S.S.A) e per le strutture Tecnico Amministrative e Sanitarie in line altresì i Responsabili/Referenti di strutture articolazione di struttura complessa (S.S.), come previste nel Piano di Organizzazione Aziendale come definito dall'art.25.3 atto aziendale approvato con deliberazione n. 391 del 29 ottobre 2010, come modificata con deliberazione n.151 del 9 giugno 2011. L'elenco dei Responsabili viene aggiornato periodicamente e riportato nel presente Documento.
I compiti di ciascuna struttura sono quelli risultanti dall'Atto Aziendale, dalla Carta dei Servizi Aziendale, nonchè dalle Carte della Qualità del Servizio, adottate dalle singole strutture e/o dai Dipartimenti ai fini del rilascio della certificazione di qualità e pubblicate sul sito Internet dell'Azienda Ospedaliera (http://www.ospedale.al.it/)
E' stata altresì realizzata una sezione dedicata alla Privacy presente sul sito Aziendale contenente il Documento aziendale vigente, il modulo per il consenso ai dati personali, l'elenco dei Responsabili del Trattamento ed i principali documenti adottati dall'Azienda in materia.
Ai sensi dell'art.4 del previgente D.Lgs.467/2001, è stato modificato il contenuto dell'informativa da rilasciare all'interessato, che deve ora prevedere, nel caso di avvenuta designazione di più di un Responsabile del trattamento, il servizio o il soggetto eventualmente preposto come "interlocutore" dell'interessato per l'esercizio dei diritti previsti dalla normativa.

Alla data di adozione del presente aggiornamento, ricoprono la posizione di "Responsabili del trattamento" i seguenti nominativi :

1.	Dott. Fabrizio FERRANDO	SSA Legale
2.	Dott. Antonio MACONI	SSA Sviluppo e Promozione Scientifica
3.	Ing. Roberta BELLINI	SSA Svil.Strategico Innovazione e Qualità
4.	Ing. Alberto PERACCHIO	SC Servizio Prevenzione e Protezione
5.	Dott.ssa Patrizia NEGRI	SC Gestione Attività Amm.ve e di supporto
6.	Dott. Luigi RIZZO	SS Affari Generali e Relazioni col Pubblico;
7.	Dr.ssa Patrizia NEBIOLO	SC Gestione e Sviluppo del Personale;
8.	Dr.ssa Enrica DEVECCHI	SC Contabilità Economica e Patrimoniale
9.	Dr.ssa Cristina CABIATI	SC Acquisti e Gestione Servizi Economali
10.	Arch. Claudio PESCE	SC Gestione Patrimonio Tecnologico e Imm.re
11.	Ing. Gianluca MAROCCO	SS Ingegneria Clinica
12.	Dott. Stefano SCARPETTA	SC Sistema Informativi- Logistici e CDG
13.	Dott. Massimo DESPERATI	SC Direzione Medica dei Presidi
14.	Dott. Alessandro CANEPARI	SS Igiene e Organizzazione Presidio C.Arrigo
15.	Dott.ssa Lorella GAMBARINI	SC SI.T.R.O.
16.	Dr.ssa Laura SAVI	SC Farmacia Ospedaliera

17.	Dott. Giovanni LOMBARDI	SC SEST 118 AL
18.	Dott.ssa Grazia LOMOLINO	SSA Controllo Infezioni Ospedaliere
19.	Dott.ssa Franca STORNINO	SSA Gestione Blocchi Operatori
20.	Dr.ssa Rita REGGIO	SSA Fisica Sanitaria
21.	Dott. Giorgio MONTOBBIO	SSA Psicologia
22.	Dott. Fabrizio CASSINI	SSA Terapia del Dolore
23.	Dott. Prospero GASTALDI	SSD Day Surgery Multispecialistico
24.	Dott. Domenico DRAGO	SSD Endoscopia Digestiva
25.	Dott.ssa Nicoletta VIVALDI	SC Anestesia e Rianimazione
26.	Dott. Giuseppe SPINOGLIO	SC Chirurgia Generale a indirizzo Oncologico
27.	Dott. Renzo PANIZZA	SC Chirurgia Plastica e Ricostruttiva
28.	Dott. Riccardo CEVOLI	SC Urologia
29.	Dott.ssa Oria TRIFOGLIO	SC Ginecologia e Ostetricia
30.	Dott.ssa Ermelinda MARTUSCELLI	SC Anestesia e Rianimazione Cv e Tor.
31.	Dott. Gianfranco PISTIS	SC Cardiologia
32.	Dott. Domenico MERCOGLIANO	SC Cardiochirurgia
33.	Dott. Maurizio MANCUSO	SC Chirurgia Toracica
34.	Dott. Mauro SALVINI	SC Chirurgia Vascolare
35.	Dott. Paolo BELLINGERI	SSD Chirurgia Maxillo Facciale
36.	Dott. Luigi Carmelo RUIZ	SC Neurologia
37.	Dott. Andrea BARBANERA	SC Neurochirurgia
38.	Dott.ssa Daniela DOLCINO	SC Oculistica
39.	Dott. Raffaele SORRENTINO	SC Otorinolaringoiatria
40.	Dott. Marco SCHIRALDI	SC Ortopedia e Traumatologia
41.	Dott. Mauro MICHELINI	SSD Dermatologia
42.	Dott. Angelo MOLINARI	SSD Malattie croniche Infiamm.dell'intestino
43.	Dott. Luca TODROS	SSD Centro di Epatologia
44.	Dott.ssa Maria MOSCATO	SC Geriatria
45.	Dott. Gabriele FERRETTI	SC Malattie Apparato Respiratorio
46.	Dott. Ivo CASAGRANDA	SC Medicina e Chirurgia d'Accettazione e d'Urgenza
47.	Dott. Piero DAVIO	SC Medicina Interna
48.	Dott. Ennio PIANTATO	SC Psichiatria-S.P.D.C.
49.	Dott.ssa Flavia SALVI	SSD Day Hospital Oncoematologico
50.	Dr.ssa Egle ANSALDI	SSD Endocrinologia e Malattie Metaboliche
51.	Dott. Pier Andrea ROCCHETTA	SSD Reumatologia
52.	Dott.ssa Flavia SALVI	SC Ematologia
53.	Dott. Alfredo MUNI	SC Medicina Nucleare
54.	Dott. Marco MANGANARO	SC Nefrologia e Dialisi
55.	Dott. Eugenio MANTIA	SC Malattie Infettive
56.	Dott. Vittorio FUSCO	SC Oncologia
57.	Dott.ssa Paola FRANZONE	SC Radioterapia
58.	Dott.ssa Anna R.COSTANTINO	SSD Serv. Trasporto Emergenza Pres.Pediatrico
59.	Dott. Luciano SANGIORGIO	SSD Urologia Pediatrica
60.	Dott. Fabrizio RACCA	SCAnestesia e Rianimazione Pediatrica
61.	Dott. Francesco VACCARELLA	SC Chirurgia Pediatrica
62.	Dott. Diego GAZZOLO	SC Neonatologia-Terapia Intensiva Neonatale
63.	Dott. Maurizio CREMONTE	SC Neuropsichiatria Infantile
64.	Dott. Fernando PESCE	SC Pediatria – SSD Mal.Infettive Pediatriche

65.	Dott. Carlo ORIGO	SC Ortopedia e Traumatologia Pediatrica
66.	Dott. Enio G. MANTELLINI	SSD Riabilitazione Cardio-Respiratoria
67.	Dott. Marco POLVERELLI	SC Medicina Fisica e Riabilitazione II livello
68.	Dott. Salvatore PETROZZINO	SC Medicina Fisica e Riabilitazione III livello
69.	Dott. Andrea ROCCHETTI	SSD Microbiologia
70.	Dott. Francesco MUSANTE	SC Radiodiagnostica - SSD Neuroradiologia
71.	Dott.ssa Patrizia RUSSO	SSD Radiodiagnostica Pediatrica
72.	Dott. Franco ZANDRINO	SSD Radiologia Interventistica
73.	Dott. Narciso MARIANI	SC Anatomia Patologica
74.	Dott. Carlo ARFINI	SC Laboratorio Analisi
75.	Dr.ssa Alida COTRONEO	SC Medicina del Lavoro
76.	Dott. Roberto GUASCHINO	SC Medicina Trasfusionale

Con deliberazione n. 1506 del 22.10.1997, il C.S.I. Piemonte (Consorzio per il Sistema Informatico – Corso Unione Sovietica, 216, Torino), è stato nominato "Responsabile del Trattamento" di tutti i dati personali relativi al personale dell'Azienda Ospedaliera di Alessandria.
In data 29.03.2000 il C.S.I. Piemonte ha comunicato all'Azienda Ospedaliera di Alessandria gli adempimenti messi in atto dall'Ente stesso in ottemperanza alla Legge 675/96 ed al D.P.R. 318/99.
Inoltre il C.S.I. Piemonte ha richiesto all'Azienda Ospedaliera di Alessandria di effettuare il controllo logico/organizzativo sulle attuali abilitazioni agli accessi ai sistemi gestiti dal C.S.I. Piemonte, in particolare:

- Definizione delle abilitazioni e delle revoche
- Definizione dei profili di accesso
- Monitoraggio della validità degli accessi
- Tempestiva comunicazione delle variazioni al C.S.I. Piemonte.

Analogamente, con deliberazione n.268 del 29.5.2001, si è provveduto a nominare Responsabili del trattamento dei dati personali, il Consorzio Nazionale dei Concessionari (C.N.C.) – Centro Elaborativo di Torino, Via Tirreno 247, e la CARALT SPA (ora EQUITALIA) con sede in Alessandria, Spalto Gamondio 1, in relazione al trattamento dei dati personali forniti dall'Azienda per la formazione dei ruoli esecutivi e per la riscossione coattiva delle entrate patrimoniali dell'Azienda, così come disciplinate dalle convenzioni approvate con deliberazioni n.2342/99 e n.13/2001, disponendo altresì a carico dei suddetti "Responsabili" l'obbligo di operare nel rispetto della vigente normativa in tema di "privacy", con particolare riferimento ai seguenti adempimenti:

a) individuazione degli Incaricati del trattamento
b) autorizzazione degli Incaricati all'eventuale trattamento di dati sensibili
c) obbligo di informativa ed eventuale raccolta del consenso degli interessati, ove necessario
d) comunicazione dei dati nei limiti di cui all'art.27 della L.675/1996
e) adozione e rispetto delle misure minime di sicurezza previste dal DPR 318/1999.

A seguito dell'entrata in vigore del D.Lgs.n.196/2003, a ciascuna delle suddette società esterne, sono stati ribaditi i principi ed i criteri ai quali attenersi, nell'ambito dei trattamenti di dati personali di pertinenza dell'Azienda Ospedaliera:

- rispetto degli obblighi previsti dal Codice in materia di protezione dei dati personali

- adozione delle misure minime di sicurezza previste dagli artt.33-35 del Codice e dall'allegato Disciplinare Tecnico
- individuazione degli incaricati del trattamento e loro autorizzazione all'eventuale trattamento di dati sensibili
- rilascio dell'informativa agli interessati ed acquisizione del loro consenso, ove necessario
- segnalazione immediata di anomalie, disfunzioni, rischi e/o criticità ravvisate nelle operazioni di trattamento di dati di pertinenza dell'Azienda Ospedaliera.

Nell'ambito del Programma Regionale di Assicurazione delle Aziende Sanitarie regionali finalizzato alla gestione dei sinistri di Responsabilità Civile interessanti l'Azienda Ospedaliera, il Responsabile del trattamento dei dati nell'ambito del Programma Regionale di Assicurazione delle Aziende Sanitarie è attualmente lo Studio IES di Milano.

Con deliberazione n.507 del 18 agosto 2009 a seguito dell'adesione dell'Azienda al progetto Rete Tumori Rari, sono stati designati Responsabili del trattamento, ciascun per la parte di rispettiva competenza le seguenti società: Telecom Italia Spa, Telbios Spa e Business-E Spa.

2.1.3 Designazione degli incaricati del trattamento

La designazione degli incaricati del trattamento viene effettuata con modalità semplificate, come peraltro previsto dallo stesso Garante con Provvedimento del 19 giugno 2008.
Di norma, infatti, tutto il personale medico, sanitario, tecnico, professionale ed amministrativo operante presso ciascuna Struttura, è individuato quale "incaricato del trattamento", nei limiti delle rispettive attribuzioni, con le funzioni ed i compiti previsti dall'art.30 del D.Lgs.n.196/2003. Pertanto, l'ambito di trattamento effettuato sia con, che senza strumenti elettronici, consentito ai singoli incaricati, è definito in stretta relazione alla struttura di assegnazione, alla qualifica ricoperta ed ai compiti assegnati dal Dirigente Responsabile, e deve intendersi automaticamente modificato in occasione di spostamenti da una struttura all'altra, anche nell'ambito del medesimo Dipartimento, ovvero in occasione di mutamenti di mansioni e/o profili funzionali.
All'interno dell'Azienda Ospedaliera esiste un sistema informatizzato di rilevazione delle presenze, che consente di estrapolare, con cadenza mensile, la dotazione organica complessiva e, di conseguenza, l'assegnazione nominativa di ogni dipendente alle varie strutture.
Di conseguenza, la lista degli incaricati viene redatta per classi omogenee e l'assegnazione scritta del soggetto (risultante dal contratto individuale di lavoro o da successive disposizioni di servizio) ad una determinata struttura, comporta la designazione quale incaricato dei trattamenti effettuati all'interno della struttura stessa.
Gli ambiti dei trattamenti consentiti ed i relativi profili di autorizzazione vengono periodicamente ed automaticamente aggiornati, sulla base delle variazioni intervenute e registrate dal programma della rilevazione presenze.

I soggetti incaricati del trattamento sono raggruppati nelle seguenti classi omogenee:
1) Dirigenza Medica e Sanitaria non medica, infermieri, tecnici sanitari e personale riabilitazione, incaricati del trattamento dei dati sensibili dei pazienti/utenti;
2) Personale ruolo amministrativo, in servizio presso strutture sanitarie, incaricati del trattamento di dati sensibili di pazienti/utenti, (ad es. personale amministrativo di S.C. Gestione Attività Amm.ve di supporto);

3) Personale del ruolo amministrativo, tecnico e professionale che trattano dati sensibili e giudiziari del personale o di terzi (ad es. SC Gestione e Sviluppo del Personale, SC Acquisti e Gestione servizi Economali, SC Gestione Patrimonio Tecnologico e Imm.re, SSA Legale, SS.Affari Generali e Relazioni col Pubblico);
4) Personale del ruolo amministrativo, tecnico e professionale, che non tratta dati sensibili e giudiziari;

La qualifica di "incaricato" spetta in relazione alle operazioni di trattamento di tutti i dati personali (dati anagrafici, recapiti telefonici, dati sensibili attinenti lo stato di salute o la vita sessuale, l'origine razziale, le convinzioni religiose o politiche, l'appartenenza a partiti o sindacati ecc.), ai quali i predetti soggetti hanno accesso, o di cui vengono a conoscenza nell'esercizio dei compiti ad essi assegnati.
Fermo restando l'obbligo del segreto d'ufficio e/o professionale che grava su tutti i dipendenti, borsisti, tirocinanti ecc... il trattamento dei dati effettuato da parte di ciascun incaricato sia con strumenti automatizzati sia su supporti cartacei, deve avvenire:

- secondo le indicazioni fornite dal responsabile del trattamento
- in modo lecito e secondo correttezza, fermo restando in ogni caso il rispetto dei generali doveri attinenti il segreto d'ufficio e professionale
- per gli scopi strettamente inerenti l'attività di competenza di ciascun incaricato
- in modo tale da assicurarne esattezza, completezza, pertinenza e non eccedenza rispetto alle finalità per le quali sono stati raccolti o trattati
- assicurando un'adeguata chiusura dei locali nei quali sono custoditi o trattati i dati personali, durante le pause di lavoro, o al di fuori del normale orario di servizio, e comunque curando di evitare la possibilità di accesso ai dati per i quali è in corso un trattamento da parte di soggetti non autorizzati, in caso di allontanamento anche temporaneo dalla postazione di lavoro
- nel rispetto delle misure di sicurezza predisposte dall'Azienda ai fini della loro conservazione.

3. Nomina dell'Amministratore del Sistema

Dall'esame dell'art.4 del D.Lgs.n.196/2003, si ricava che, almeno nominalmente, il legislatore, in un'ottica di semplificazione degli adempimenti, non ha ritenuto di riproporre la figura dell'Amministratore di Sistema.
Il nuovo Codice si limita a definire unicamente le figure del Responsabile e dell'Incaricato del trattamento, lasciando alla libera determinazione di ciascun Titolare, l'identificazione e l'assegnazione di attività e responsabilità a specifici ruoli all'interno della propria organizzazione.
Tuttavia, il Garante, con provvedimento del 27 novembre 2008, ha ritenuto indispensabile fornire a tutti i titolari di trattamenti di dati personali, una serie di indicazioni e/o di prescrizioni relative alla figura dell'Amministratore di sistema, o ad altre ad essa assimilabili (database administrator, network administrator) evidenziando la particolare criticità delle attività svolte da questi soggetti.
Alla luce di quanto sopra, l'Azienda :

1) ha individuato quali propri Amministratori di sistema:
- il Dr. Stefano Scarpetta, Dirigente SC Servizi Informativi Logistici e CDG
- il Dr. Roberto Pagella, Responsabile WEB Master
in quanto in possesso delle competenze tecniche e dell'esperienza necessarie ad assicurare il pieno rispetto delle vigenti disposizioni in materia di privacy, ed in particolare degli aspetti legati alla sicurezza nel trattamento dei dati;

2) ha confermato i compiti e le attribuzioni spettanti all'Amministratore di sistema, come sopra delineati e precisamente:

- 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 (operatori backup e recovery) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella qualità di "amministratore del sistema") tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste

3) in adempimento al provvedimento del 25 giugno 2009 recante le modifiche al provvedimento del Garante sulle Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre 2008, l'Azienda Ospedaliera si è dotata di software che permette da parte del Garante l'accesso diretto per la verifica della rispondenza delle misure di sicurezza adottate agli standard previsti per legge, nonchè la segnalazione di eventuali criticità e/o di ulteriori misure attuabili per incrementare il livello di sicurezza aziendale nel trattamento dei dati;

4) a seguito del provvedimento del 27 novembre 2008 del Garante per la protezione dei dati personali, e dei chiarimenti dallo stesso resi sul proprio sito web, ha provveduto a richiedere alle aziende fornitrici di software l'individuazione dei soggetti dalle stesse addetti all'espletamento delle suddette funzioni di "Amministratore di base dati" e "Amministratore di sistema software complesso".

4. Disposizioni in tema di privacy per i servizi esternalizzati.

Sono stati incaricati del trattamento dei dati personali i Legali Rappresentati delle seguenti ditte che gestiscono servizi esterni relativi a front office e archiviazione:

OGGETTO	DITTA AGGIUDICATARIA
servizi di movimentazione merci squadra e cartelle cliniche	COOP. SOC. LAVORO LIBERAZIONE
servizio portineria presso Borsalino	COOP. SOC. MARCONDIRO
servizio di call center prenotazioni	GESAN
servizio archiviazione documenti	F.D.M. SRL
servizio segreteria libera professione	COOP. SOC. AS.PER
servizio front office Gardella	COOP. SOC. AS.PER
servizio di noleggio presidi	ZUCCATO HC SRL / HILL ROM SPA

antidecubito

Family Room FONDAZIONE RONALD MC DONALD

5. Misure logiche

5.1 Inventario del Software

Il Centro Elaborazione Dati ha segnalato la presenza dei seguenti pacchetti software:

Protocollo Generale (Italcom)
Gestione Amministrativa (Engisanità)
Gestione Stipendi (CSI)
Anatomia Patologica (Engisanità)
Immunotrasfusionale (Engisanità)
Gestione personale (Cabril)
Laboratorio analisi (Siemens)
Nefrologia (Sined)
Emodinamica Fuji)
Cardiologia (3A Sistemi)
Radiologia (Fuji)
Centro Unificato Prenotazione e Accettazione ospedaliera e registro operatorio forniti da C.S.I.
Delibere (Engisanità)
Terapia Intensiva Neonatale (Enicq)
Ginecologia diagnostica (Fuji)

5. 2. Trattamento dei dati personali effettuato con strumenti elettronici o comunque automatizzati

Il Disciplinare Tecnico contenuto nell'Allegato B al Codice ha integralmente sostituito il previgente Regolamento approvato con il D.P.R. n.318/1999, nei cui confronti appare decisamente più evoluto e moderno.
A parte le innovazioni di carattere tecnico che comportano un innalzamento del livello "minimo" di sicurezza, resta confermata la precipua finalità di garantire il diritto alla riservatezza degli interessati attraverso una serie di misure che garantiscano la cosiddetta "security" della rete informatica aziendale.
Nell'ambito dei trattamenti effettuati con strumenti elettronici, il Disciplinare Tecnico non ripropone la previgente distinzione in tre sottocategorie (elaboratori stand alone, in rete privata e in rete pubblica).
Ove possibile, le apparecchiature non tecnicamente idonee verranno dismesse e sostituite con nuovo hardware avente le caratteristiche tecniche necessarie.
Nelle more, è previsto che ciascun Responsabile del trattamento, al fine di garantire l'integrità dei dati trattati, verifichi il rispetto delle misure minime di sicurezza (adozione di una password individuale, salva-schermo con parola d'accesso, antivirus, salvataggi e/o duplicazioni periodiche dei dati, sostituzione periodica della passwords, ecc..).
I client mantengono i dati di lavoro su server aziendale, che rispetta i dettami del testo di legge.
I dati personali degli utenti, qualora esistano, sono mantenuti in locale sulle postazioni e non sono

oggetto di "security" aziendale.
Con deliberazione n.335 del 29.3.2000, è stata disposta una prima serie di misure minime di sicurezza da osservare nel trattamento di dati effettuato con strumenti elettronici o comunque automatizzati.
Dall'anno 2013 presso il presidio Gardella è stato implementato il programma informatizzato di raccolta del consenso al trattamento dati personali effettuato all'atto della prenotazione dei prelievi ai sensi della vigente normativa.

5. 3 Accesso ad Internet

La connessione ad Internet è tramite una linea SHDSL a (2 Mbit) 10 Mbit/s – Fastweb.
E' stata allegata ai cedolini stipendiali di febbraio 2001 di tutti i dipendenti, una comunicazione del Direttore Generale relativa alle modalità di accesso e di corretto utilizzo di Internet.
A seguito dell'adozione da parte del Garante per la Protezione dei dati Personali del Provvedimento in data 1 marzo 2007 e pubblicato sulla Gazzetta Ufficiale del 10 marzo 2007 n.58, in materia di trattamento dei dati relativo all'utilizzo da parte dei lavoratori di strumenti elettronici e, segnatamente, di Internet e posta elettronica, ed in ottemperanza a quanto previsto dalla Direttiva n. 2 del 26 maggio 2009 del Dipartimento della Funzione Pubblica, con deliberazione n. 53 dell'11 febbraio 2010 è stato approvato il Disciplinare sull'uso della posta elettronica e della rete internet.

5. 4 Codici Identificativi/Utente e Password

Conformemente a quanto previsto dall'art.34 comma 1 lett. a) del D.Lgs.196/2003, ad ogni incaricato del trattamento di dati con strumenti elettronici, corrisponde un sistema di autenticazione informatica con l'assegnazione di un codice identificativo.
Tutti gli incaricati che usano un PC hanno un utente ed una password nominativi di cui sono responsabili, e sono stati eliminati utenti e password generici a disposizione di più utenti di uno stesso servizio. Se un utente con la relativa password non venisse usato per un periodo di sei mesi, questo deve essere disattivato.
La password è personale e segreta, fatta salva l'ipotesi prevista dal punto 10 del Disciplinare Tecnico allegato al D.Lgs.196/2003, che consente al Titolare di adottare un sistema di "custodia delle copie delle credenziali di autenticazione" per accedere ai singoli elaboratori, alle seguenti condizioni:
1) che abbia adottato misure idonee e preventive disposizioni per individuare le modalità di accesso;
2) che l'accesso sia determinato dalla prolungata assenza o impedimento dell'incaricato;
3) che l'accesso stesso sia indispensabile ed indifferibile e determinato per esclusive esigenze di operatività e sicurezza del sistema.
Il personale del CED, su autorizzazione del Dirigente Responsabile della Struttura provvede a "disabilitare" (reset) la password dell'incaricato e con una password provvisoria accede al PC, nel rispetto della privacy del dipendente, esclusivamente e per il tempo strettamente necessario all'effettuazione delle operazioni indispensabili a garantire l'operatività e la sicurezza del sistema.
Al termine dell'intervento, il CED nuovamente sostituisce la password provvisoria. L'incaricato assente, oltre ad esserne stato informato, al suo rientro dovrà contattare il CED per una nuova password per accedere al suo PC.
Ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, sono state fornite a ciascun incaricato le istruzioni per provvedere all'autonoma sostituzione della password, con le periodicità previste per legge.
In merito al contenuto delle password personali, con comunicazione del 19 ottobre 2010, il CED ha ricordato a tutto il personale le principali regole da seguire per assicurare il più ampio livello di

sicurezza.

In particolare:

- le password devono essere lunghe 8 o più caratteri
- non dovranno contenere più di due caratteri consecutivi del nome completo dell'utente o del nome dell'account utente
- devono contenere caratteri appartenenti ad almeno tre delle quattro categorie seguenti:
- Caratteri maiuscoli dell'alfabeto inglese (A-Z)
- Caratteri minuscoli dell'alfabeto inglese (a-z)
- Cifre decimali (0-9)
- Caratteri non alfabetici, ad esempio !, $, #, %

I requisiti di complessità vengono verificati al momento della creazione o della modifica delle password, la cui durata è stata fissata in 90 giorni.
Una volta assegnati i singoli codici identificativi, per accedere alla rete sarà predisposto un sistema per garantire che lo stesso codice non possa, neppure in tempi diversi, essere assegnato a persone diverse.
Il Server principale è custode di tutti i codici identificativi e delle parole chiave degli utenti collegati in rete. La Parola Chiave del Server è custodita dagli Amministratori di Sistema.
Gli operatori manutentivi del sistema, facenti parte del Ced, hanno la possibilità di effettuare operazioni di disattivazioni della password degli utenti in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore a sei mesi.

5. 5 Programmi Antivirus

E' stata effettuata l'installazione su tutte le postazioni di lavoro di software Antivirus per la protezione contro il rischio di intrusione, con aggiornamento degli stessi a cadenza settimanale.
E' stato inoltre disposto che il caricamento sui PC aziendali di programmi o dati non autorizzati, avvenga solo con il preventivo assenso del personale del CED, e che venga prestata la massima cautela nell'apertura di files o di allegati di posta elettronica di dubbia provenienza.

5. 6 Firewall

E' stata effettuata l'installazione di un 'Firewall' in grado di controllare l'accesso alle reti, intercettando tutti i messaggi in entrata e in uscita e garantendo quindi la rete aziendale contro l'intrusione dall'esterno.

5. 7 Reimpiego dei supporti di memorizzazione

Tutte le informazioni precedentemente contenute sui supporti di memorizzazione vengono cancellate in modo permanente prima di un loro eventuale reimpiego.

5. 8 Procedure di Backup e di disaster recovery

Tra le misure di sicurezza adottate dall'Azienda con deliberazione n.335/2000 e n.30/2002 è stato disposto che ciascun dipendente provveda all'effettuazione di duplicazione dei dati AZIENDALI e di salvataggi frequenti dei dati AZIENDALI contenuti su PC
Le procedure di Backup sono impostate in modo da eseguire il salvataggio in modalità automatica.

Vengono eseguite le procedure di "export" dei vari Database e scaricati su nastri (LTO) diversi, ogni notte. I nastri sono utilizzati a rotazione ogni giorno della settimana. I nastri vengono conservati in un armadio chiuso al di fuori della stanza del Server.
Il punto 23 del Disciplinare Tecnico impone l'adozione di "*idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni*" (cd. procedure di disaster recovery).
E' stato acquisito tutto il materiale hardware e software necessario ad assicurare il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici nel termine massimo di sette giorni fissato dal punto 23 del Disciplinare.
Inoltre nell'ambito del Sistema Aziendale Qualità la Struttura Sistemi Informativi ha emesso la quinta revisione dell'Istruzione Operativa ISII 04 Attività di backup dei Server dell'Azienda, al fine di descrivere le attività e gli interventi per assicurare la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività, in atti c/o la stessa Struttura nonché in visione su Intranet.

In adempimento alle disposizioni del nuovo Codice di Amministrazione Digitale nel corso dell'anno l'Azienda svilupperà i contenuti di tali istruzioni interne in piani di emergenza che comprenderanno un Piano di continuità operativa e un Piano di Disaster Recovery da sottoporre al parere di fattibilità tecnica di DigitPA

6. Aggiornamenti e auditing

Il presente Documento è oggetto di periodico aggiornamento.
In occasione dell'operazione di aggiornamento di cui sopra, l'Azienda Ospedaliera provvede ad effettuare le verifiche dei dispositivi organizzativi ed in particolare dell'efficacia delle misure minime di sicurezza intraprese e riportate nel presente Documento.

Ulteriori verifiche possono essere predisposte con periodicità infrannuale, al verificarsi di eventi "sentinella" segnalati dai Responsabili del Trattamento, o per effetto dell'individuazione di nuove tipologie di rischi precedente non valutate.

Inoltre è stato adottato con deliberazione n. 257 del 19/09/2011 il Regolamento Aziendale in materia di Protezione dei dati Personali, anch'esso pubblicato sul sito aziendale all'indirizzo http://10.70.0.114:8080/AreaRiservata/News_Doc/RegolamentoPrivacy.pdf

Il documento Aziendale per la sicurezza in vigore è pubblicato sul sito aziendale all'indirizzo:
http://10.70.0.114:8080/AreaRiservata/News_Doc/DocumentoProgrammaticoperlaSicurezza.pdf

Regione Piemonte

Azienda Ospedaliera "SS. Antonio e Biagio e C. Arrigo"

Alessandria

Deliberazione del DIRETTORE GENERALE n° **77** del **04/03/2014** (ai sensi della D.G.R. n.18 - 3728 del 27.4.2012)

CERTIFICATO DI PUBBLICAZIONE

La presente deliberazione viene pubblicata all'Albo Pretorio on-line dell'Azienda Ospedaliera "SS. Antonio e Biagio e C. Arrigo" per 15 giorni consecutivi a decorrere dal 13/03/2014

Alessandria, lì 13/03/2014

Il Funzionario Incaricato
(Dr. Luigi Rizzo)

- Esecutiva dal: 23/03/2014

Trasmessa:

- Al Presidente Collegio Sindacale in data: 13/03/2014

- Alla Giunta Regionale in data:
- Richiesta chiarimenti in data:
- Ricevuti chiarimenti in data: