

**Estratto da:**

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

Edizione 03/2009

(.....)

**2. ELENCO DEI TRATTAMENTI (REGOLA 19.1)**

Con nota prot.n.14560/C del 29.6.1998, l'Azienda Ospedaliera di Alessandria ha effettuato al Garante per la protezione dei dati personali, la notificazione in forma semplificata prevista dagli artt.7, 16 e 28 della Legge n.675/1996.

Alla luce di quanto disposto dagli artt.37 e 38 del D.Lgs.n.196/2003, l'Azienda, in qualità di Titolare del trattamento dei dati ex art.28 del Codice, ha effettuato in data 29 aprile 2004 una nuova notificazione al Garante, che è stata inserita nel Registro dei Trattamenti (Codice C.U.N. 0000-0053-4887-4458).

Al fine di adempiere a quanto stabilito dalla Regola 19.1 del Disciplinare Tecnico, era stato richiesto a ciascun Responsabile del trattamento di compilare un apposito questionario (allegato 1), con le seguenti finalità:

1. Individuazione di tutte le banche dati esistenti, contenenti e non dati sensibili, per comprendere in dettaglio il flusso dei dati all'interno dell'Azienda;
2. Attribuzione di un nome a ciascuna banca dati e definizione del suo contenuto;
3. Individuazione e definizione della finalità del trattamento;
4. Individuazione delle misure di controllo in atto per la salvaguardia della sicurezza dei dati.

In questo modo è stato possibile ottenere una mappatura di tutte le banche dati e quindi l'elenco dei trattamenti di dati personali effettuati all'interno di ciascuna Struttura sia su base informatica che cartacea, conformemente alle disposizioni del Disciplinare Tecnico.

I dati ottenuti sono oggetto di periodico aggiornamento a cura dei vari responsabili del trattamento.

La raccolta delle informazioni aggiornate pervenute, relative al flusso dei dati all'interno dell'Azienda è sintetizzata nell'allegato 2, mentre nell'allegato 3 sono elencati tutti i trattamenti censiti.

L'esame di tale documentazione consente di distinguere tra le diverse tipologie di dato:

- su base cartacea, sensibili
- su base cartacea, non sensibili
- su base elettronica, sensibili
- su base elettronica, non sensibili.

I questionari richiedevano anche al compilatore la registrazione delle misure primarie di sicurezza applicate: in sostanza l'uso di chiavi di accesso ai dati, sia fisiche (per gli archivi cartacei) che elettroniche (passwords).

Le situazioni generalmente riscontrabili sono le seguenti:

- i dati contenuti su base cartacea sono conservati nell'ambito di ciascuna struttura in armadi e/o locali costantemente presidiati durante l'orario di servizio e chiusi a chiave negli orari e nelle giornate non lavorative;
- in pochissimi casi convivono banche dati totalmente o parzialmente duplicate, sia su base cartacea che elettronica;
- trattandosi in gran parte di dati attinenti la salute dei pazienti, soggetti a conservazione illimitata nel tempo, viene distrutta solo documentazione di natura amministrativa, nel rispetto dei termini e delle procedure adottate dall'Azienda Ospedaliera per la conservazione e lo scarto degli atti d'archivio;
- i dati vengono talvolta restituiti/inviati al mittente, ossia al paziente/utente, sottoforma di cartelle cliniche, referti e/o documentazione attestante la prestazione sanitaria erogata dall'Azienda;
- i dati possono essere trasmessi all'esterno dell'Azienda, ma in questo caso solo per adempimenti di natura istituzionale o previo consenso dell'interessato;
- le informazioni elettroniche sono conservate su PC collegati in rete, e quindi più facilmente controllabili dall'Amministratore di sistema;
- non sono stati riscontrati casi di PC stand alone collegati a reti esterne (ad esempio ad Internet tramite modem);
- la cultura della 'privacy' è generalmente diffusa e viene evitata l'inutile duplicazione e trasmissione di dati sensibili;
- i dati sensibili attinenti lo stato di salute sono generalmente raccolti direttamente dal personale dell'Azienda nel contatto con i pazienti e con operatori sanitari interni;
- la maggior parte delle fonti e dei destinatari delle informazioni sono interni all'Azienda;
- le fonti ed i destinatari esterni sono normalmente enti pubblici e raramente soggetti privati.

Si ricorda che la maggior parte delle relazioni con l'esterno sono dettagliatamente regolamentate dalla Direzione Medica dei Presidi, in particolare i rapporti con i soggetti privati, quali aziende farmaceutiche, per sperimentazioni.

Con D.P.G.R. n.3/R dell'11.5.2006, come rettificato con D.P.G.R. n.4/R del 4.12.2006, la Regione Piemonte, secondo quanto previsto dall'art.20 comma 2 del D.Lgs.196/2003, ha adottato il Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della regione e degli enti da essa vigilati, tra cui le AA.SS.RR., con particolare riferimento all'individuazione delle operazioni eseguibili e della tipologia di dati sensibili trattati per il perseguimento di finalità istituzionali.

Detto regolamento, direttamente ed immediatamente operante, senza necessità di alcun atto formale di recepimento, è stato trasmesso a tutti i responsabili del trattamento per gli adempimenti di rispettiva competenza.

### **3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ (REGOLA 19.2)**

#### **3.1. 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 DPS
- riferisce nella relazione accompagnatoria del bilancio d'esercizio predisposta dalla SC Contabilità e Finanza, dell'avvenuta redazione o aggiornamento del DPS
- 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

#### **3.2. 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 agli artt. 1 comma 2 lett. e) ed 8 della previgente Legge 675/96, ora contemplati dall'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.), come previste nel Piano di Organizzazione Aziendale.

L'elenco dei Responsabili viene aggiornato periodicamente e riportato nel presente Documento Programmatico sulla Sicurezza.

I compiti di ciascuna struttura sono quelli risultanti dall'Atto Aziendale, dalla Carta dei Servizi Aziendale, nonché 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/>).

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.

Con provvedimento del 25.2.2002, il Commissario ha individuato detto servizio nell'URE-URP, che pertanto viene indicato nei nuovi moduli di informativa e contestuale rilascio del consenso, come il soggetto presso il quale ciascun interessato potrà conoscere i nominativi dei vari Responsabili del trattamento, per l'esercizio dei diritti ora previsti dall'art.7 del Codice.

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

1. Dott. Fabrizio FERRANDO	Affari Generali e Legale
2. Dr.ssa Enrica DEVECCHI	Amministrazione del Personale
3. Dr.ssa Patrizia NEGRI	Contabilità e Finanza
4. Dott.ssa Delfina LEGORA	Controllo di Gestione
5. Dr.ssa Patrizia NEBIOLO	Organizzazione e Sviluppo delle Risorse Umane
6. Dott.ssa Cristina CHIALVI	Relazioni con il Pubblico
7. Dott.ssa Roberta BELLINI	Sistema Qualità (SS)
8. Dott. Stefano SCARPETTA(CSI delibera n.281/08)	Sistema Informativi- ICT
9. Ing. Alberto PERACCHIO	Servizio Prevenzione e Protezione
10. Dr.ssa Cristina CABIATI	Acquisti-Logistica
11. Ing. Giovanni POGGIALINI	Ingegneria Clinica
12. Dr. Andrea VANNER	Patrimonio (SSD)
13. Arch. Claudio PESCE	Tecnico
14. Dott. Giovanni LOMBARDI	Centrale Operativa Emergenza 118
15. Dott.ssa Grazia LOMOLINO	Controllo Infezioni Ospedaliere (SS)
16. Dott. Massimo DESPERATI	Direzione Medica dei Presidi
17. Dr.ssa Laura SAVI	Farmacia Ospedaliera
18. Dr.ssa Rita REGGIO	Fisica Sanitaria (SS)
19. Dr.ssa Alida COTRONEO	Medicina del Lavoro
20. Dott. Ennio PIANTATO	Psichiatria-S.P.D.C.
21. Dott. Giorgio MONTOBBIO	Psicologia (SS)
22. Dr.ssa Graziella GIAMBONE	Servizio Infermieristico – S.I.T.R.e P.O.
23. Dott. Pier Giacomo BETTA	Anatomia e Istologia Patologica
24. Dott. Augusto PERGOLO	Anestesia e Rianimazione
25. Dott. Giuseppe CAROSIO	Cardiologia
26. Dott. Dante MEDICI	Cardiochirurgia
27. Dott. Giuseppe SPINOGLIO	Chirurgia Generale
28. Dott. Paolo BELLINGERI	Chirurgia Maxillo Facciale (SSD)
29. Dott. Renzo PANIZZA	Chirurgia Plastica e Ricostruttiva
30. Dott. Maurizio MANCUSO	Chirurgia Toracica
31. Dott. Mauro SALVINI	Chirurgia Vascolare
32. Dott.ssa Flavia SALVI	Day Hospital Oncoematologico (SSD)
33. Dott. Prospero GASTALDI	Day Surgery Multidisciplinare (SSD)
34. Dott. Mauro AZZINI	Dermatologia in qualità di Direttore del Dipartimento Internistico
35. Dott. Giuseppe ROSTI	Endocrinologia e Malattie Metaboliche
36. Dott. Domenico DRAGO	Endoscopia Digestiva (SSD)
37. Dott. Alessandro LEVIS	Ematologia
38. Dott. Luca TODROS	Gastroenterologia
39. Dott.ssa Franca STORNINO	Gestione Blocchi Operatori (SSD)
40. Dott. Enzo LAGUZZI	Geriatrics
41. Dott. Enrico ROVETTA	Ginecologia e Ostetricia
42. Dott. Carlo ARFINI	Laboratorio Analisi
43. Dott. Gabriele FERRETTI	Malattie Apparato Respiratorio
44. Dott. Mauro AZZINI	Malattie Infettive
45. Dott. Marco POLVERELLI	Medicina Fisica e Riabilitazione II livello
46. Dott. Salvatore PETROZZINO	Medicina Fisica e Riabilitazione III livello

47. Dott. Roberto GUASCHINO	Medicina Trasmfusionale
48. Dott. Piero DAVIO	Medicina Interna
49. Dott. Ivo CASAGRANDA	Medicina e Chirurgia d'Urgenza
50. Dott.ssa Ornella TESTORI	Medicina Nucleare
51. Dott. Andrea ROCCHETTI	Microbiologia (SSD)
52. Dott. Gian Vito VERONESI	Nefrologia e Dialisi
53. Dott. Emilio URSINO	Neurologia
54. Dott. Pietro Primo VERSARI	Neurochirurgia
55. Dott. Giuseppe ROLANDI	Neuroradiologia (SSD)
56. Dott.ssa Daniela DOLCINO	Oculistica
57. Dott. Marco SCHIRALDI	Ortopedia e Traumatologia
58. Dott. Raffaele SORRENTINO	Otorinolaringoiatria
59. Dott. Guido BOTTERO	Oncologia
60. Dott. Enio G. MANTELLINI	Riabilitazione Cardio-Respiratoria (SSD)
61. Dott. Pier Andrea ROCCHETTA	Reumatologia (SSD)
62. Dott. Francesco MUSANTE	Radiodiagnostica
63. Dott. Francesco MUSANTE	Radiologia Interventistica, in qualità di Direttore del Dipartimento di Diagnostica per Immagini
64. Dott.ssa Paola FRANZONE	Radioterapia
65. Dott. Augusto PERGOLO	Terapia del Dolore, in qualità di direttore Dipartimento Anestesia e Rianimazione Terapia Intensiva e Rianimazione (SSD)
66. Dott.ssa Nicoletta VIVALDI	Urologia
67. Dott. Riccardo CEVOLI	Urologia
68. Dott.ssa Anna R.COSTANTINO	Anestesia e Rianimazione Pediatrica
69. Dott. Pier Luigi SEYMANDI	Chirurgia Pediatrica
70. Dott. Silvano GANDINI	Malattie Infettive Pediatriche (SSD)
71. Dott. Diego GAZZOLO	Neonatologia-Terapia Intensiva Neonatale
72. Dott. Dante BESANA	Neuropsichiatria Infantile
73. Dott. Carlo ORIGO	Ortopedia e Traumatologia Pediatrica
74. Dott. Fernando PESCE	Pediatria
75. Dott.ssa Patrizia RUSSO	Radiodiagnostica Pediatrica (SSD)
76. Dott.ssa Anna R.COSTANTINO	S.T.E.N. - Servizio Trasporto Emergenza Neonatale (SSD)
77. Dott. Luciano SANGIORGIO	Urologia Pediatrica (SSD)

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, ed in conformità a quanto previsto dalla Regola 19.7 del Disciplinare Tecnico, 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.

Da ultimo, con deliberazione n. 243 del 10 marzo 2008, la Faro Assicurazioni di Genova, la Rappresentanza Generale per l’Italia di Zurich Insurance e lo Studio Vaiano di Torino, ciascuno per quanto di rispettiva competenza, sono stati nominati Responsabili del trattamento dei dati nell’ambito del Programma regionale di assicurazione delle Aziende Sanitarie regionali valido per il triennio 2008/2010, ai fini della gestione dei sinistri di Responsabilità Civile interessanti l’Azienda Ospedaliera.

### **3.3. 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 reparto, CUP)
- 3) Personale del ruolo amministrativo, tecnico e professionale che trattano dati sensibili e giudiziari del personale o di terzi (ad es. SC Personale, SC Affari Generali e Legale, SC Acquisti e Logistica, SC Tecnico, SC URP);
- 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, ai quali i predetti soggetti hanno accesso, o di cui vengono a conoscenza nell'esercizio dei compiti ad essi assegnati (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.).

Fermo restando l'obbligo del segreto d'ufficio e/o professionale che grava su tutti i dipendenti, 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.

(.....)

### **3.4.1. Nomina dell'Amministratore del Sistema**

Con deliberazione n.335 del 29.03.2000 il Dr. Roberto Pagella, Responsabile della SOS Sistema Informativo d'Azienda era stato nominato Amministratore di Sistema, ai sensi dell'art.1 lett.c) del D.P.R. 318/99 con compiti di:

- Protezione dell'Informazione automatizzata e di conseguenza di dati, applicazioni, sistemi e reti;
- Verifica dell'utilizzo e della corretta funzionalità dei sistemi e delle applicazioni;
- Gestione delle manutenzioni ordinarie e straordinarie.

Con deliberazione n.281 del 14 marzo 2008 è stato affidato al CSI Piemonte il servizio di coordinamento e gestione del Sistema Informativo aziendale, nonché di supporto alla gestione dell'infrastruttura tecnico-informatica, nel cui ambito è altresì prevista la responsabilità complessiva dell'efficacia, sicurezza ed efficienza del Sistema Informativo.

In sede di assunzione dell'incarico il CSI Piemonte ha dichiarato di operare in conformità ai principi fissati dal D.Lgs.196/2003.

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) individua quali propri Amministratori di sistema:

- il Dr. Stefano Scarpetta, Responsabile SC Servizi Informatici e Informativi – ICT
- il Dr. Roberto Pagella, Responsabile SS Gestione Base dati aziendale

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

- Protezione dell'Informazione automatizzata e di conseguenza di dati, applicazioni, sistemi e reti;
- Verifica dell'utilizzo e della corretta funzionalità dei sistemi e delle applicazioni;
- Gestione delle manutenzioni ordinarie e straordinarie.

3) dispone che l'operato degli amministratori di sistema sia soggetto a verifica almeno annuale, che dovrà avvenire attraverso la predisposizione di appositi report periodici da

trasmettere alla Direzione Generale, riguardanti la rispondenza delle misure di sicurezza adottate agli standard previsti per legge, nonché la segnalazione di eventuali criticità e/o di ulteriori misure attuabili per incrementare il livello di sicurezza aziendale nel trattamento dei dati.

#### **4. ANALISI E VALUTAZIONE DEI RISCHI (REGOLA 19.3)**

Per una corretta individuazione delle misure di sicurezza da adottare, si è resa necessaria una preliminare attività di analisi e valutazione dei rischi, con ciò intendendosi tutte quelle situazioni, eventi o condotte potenzialmente dannosi e che quindi possono determinare rischi di perdita, distruzione o trattamento illecito dei dati personali.

Il numero di elementi di rischio, per il quale si rende necessaria l'attuazione di adeguate misure di sicurezza, dipende dal grado di esposizione al rischio che si è disposti a tollerare.

Si può identificare, così, una soglia che suddivida i rischi in:

- ACCETTABILI, per i quali non è conveniente realizzare alcuna misura di sicurezza;
- NON ACCETTABILI, per i quali invece è necessario determinare un certo numero di misure di sicurezza, che dovranno essere implementate secondo un piano ben definito.

L'esame dei rischi è stato fatto anche in relazione alla natura dei dati, distinguendo tra i dati personali comuni e particolari (sensibili, giudiziari), ed in relazione alle caratteristiche del trattamento.

I rischi esaminati sono stati individuati, classificati e descritti nei seguenti principali raggruppamenti:

##### **4.1. Rischi ambientali**

Sono considerati rischi ambientali quelli legati alla collocazione geografica dei luoghi dove sono conservate e trattate le diverse informazioni.

##### **4.1.1 Rischio sismico**

A seguito dell'Ordinanza del Presidente del Consiglio dei Ministri n. 3274 del 20 marzo 2003, recante 'Primi elementi in materia di criteri generali per la classificazione sismica del territorio nazionale e di normative tecniche per le costruzioni in zona sismica', è stata introdotta una nuova classificazione sismica del territorio nazionale articolata in 4 zone, le prime tre delle quali corrispondono alle zone di sismicità alta (S=12), media (S=9) e bassa (S=6), mentre per la zona 4, di nuova introduzione, si dà facoltà alla regioni di imporre l'obbligo della progettazione antisismica.

Per quanto riguarda la Regione Piemonte sono classificati in zona due 41 Comuni, (nessuno in provincia di Alessandria), mentre nella zona tre che, secondo la nuova classificazione è considerata debolmente sismica, entrano 168 comuni (46 n provincia di Alessandria).

Gli altri restanti 1000 comuni, tra cui il comune di Alessandria, sono classificati in zona 4, a bassa sismicità: nella zona 4 non viene introdotto l'obbligo della progettazione antisismica, tranne che per interventi che interessano alcune tipologie di edifici

strategici.

#### **4.1.2 Rischio alluvionale**

La città di Alessandria, circondata da due corsi d'acqua di rilevante portata (Tanaro e Bormida) è stata colpita nel 1994 da importante evento alluvionale che ha interessato anche fondi e seminterrati della struttura ospedaliera.

Precauzionalmente, gli archivi e le zone di lavoro sono state portate a livelli più elevati, mentre le misure adottate di bonifica dei corsi d'acqua e di innalzamento degli argini hanno dimostrato, al momento di essere adeguate ed hanno evitato il ripetersi dei fenomeni.

#### **4.2 Integrità dei dati**

Il concetto di "integrità" è stato riferito alla correttezza dei dati. Pertanto, le informazioni non devono essere alterabili da incidenti o abusi.

L'esame dei rischi possibili circa le minacce all'integrità dei dati sono stati classificati in:

- rischi di natura accidentale;
- rischi da programmi
- rischi di carattere volontario.

##### **4.2.1 Rischi di natura accidentale**

Per i dati trattati elettronicamente riguardano l'involontaria sovrascrittura o distruzione dei dati, imputabili ad azioni umane errate oppure a guasti, malfunzionamenti o interruzioni nel funzionamento delle apparecchiature dedicate alla memorizzazione.

Rientrano in questa categoria i rischi dovuti a:

- comandi applicativi errati (a causa di applicazioni non testate in maniera sufficiente) o eseguiti da personale non sufficientemente addestrato);
- malfunzionamenti hardware;
- deterioramento nel tempo dei supporti di memorizzazione e del mezzo fisico che li ospita;
- software pericoloso, in particolare virus dei computer;
- mancanza o interruzione di alimentazione elettrica, dovuta a black-out del fornitore del servizio.

Per i dati trattati su supporto cartaceo rientrano in questa categoria i rischi dovuti a :

- distruzione di documentazione per incendio, allagamento, umidità
- errori umani nell'archiviazione cartacea dei documenti (scambio di documentazione).

Per i dati trattati verbalmente rientrano in questa categoria i rischi dovuti a :

- comunicazioni non supportate da documentazione oggettiva (scambio di paziente)

##### **4.2.2 Rischi da programmi**

I rischi connessi alla diffusione dei virus e dei programmi pericolosi sono stati così individuati :

- perdita di file;
- perdita di spazio utilizzabile nelle memorie;
- cattivi funzionamenti del sistema;
- degrado delle prestazioni del sistema;
- impossibilità di utilizzo del sistema;

I virus ed i programmi pericolosi potrebbero penetrare nei computer aziendali tramite:

- supporti infettati provenienti da terzi;
- supporti infettati importati dai dipendenti senza l'autorizzazione dell'azienda;
- file scambiati in rete.

#### **4.2.3 Rischi di carattere volontario**

Sono le alterazioni dell'integrità conseguenti ad un'eventuale azione volontariamente posta in essere allo scopo di leggere modificare, inserire o distruggere volontariamente e indebitamente dati riservati.

Per i dati trattati elettronicamente Riguardano la sovrascrittura o distruzione dei dati, imputabili ad azioni umane

- comandi operativi pericolosi (es. cancellazioni, copie)
- interventi sull'hardware (es: spegnimenti volontari delle unità di elaborazione, furti di supporti di memorizzazione, installazioni PC e o Notebook non autorizzati, utilizzo di floppy o chiavi USB di dubbia provenienza)
- installazione di software pericoloso
- “furto di identità elettronica”
- modifica non autorizzata di dati e documenti
- saturazione della banda (downloads non consentiti)

Per i dati trattati su supporto cartaceo rientrano in questa categoria i rischi dovuti a :

- distruzione o furto di documentazione,
- modifica volontaria di documentazione da parte di personale non autorizzato o per scopi non leciti

Per i dati trattati verbalmente rientrano in questa categoria i rischi dovuti a :

- comunicazioni carenti o erronee agli interessati e a terzi per cui esista chiaro consenso

### **4.3 Riservatezza dei dati**

Per “riservatezza” dei dati si intende il dovuto e necessario riserbo sulle informazioni proteggendole da eventuali accessi e/o divulgazioni non autorizzate, consentendone l'utilizzo ed il trattamento solamente ai soggetti incaricati.

Gli eventi controllati posti in relazione al rischio di accessi non autorizzati sono stati determinati sulla base delle seguenti fattispecie :

- rischi di accessi fraudolenti dall'interno;
- rischi di accessi fraudolenti dall'esterno;

#### **4.3.1 Rischi di accessi fraudolenti dall'interno**

Per i dati trattati elettronicamente rientrano in questa categoria i rischi dovuti a :

- “profilo” di autorizzazione all'accesso non corrispondenti al ruolo assegnato o non aggiornato con conseguente attribuzione di “privilegi” di accesso eccessivi;

- “inferenza”, (indebita conoscenza indiretta di dati attraverso combinazioni di informazioni tra loro correlate);
- utilizzo indebito dei privilegi di “Amministratori di Sistema” per l’accesso ad archivi;
- “furto di identità elettronica” di un dipendente autorizzato all’accesso ai sistemi;
- “manomissione” delle autorizzazioni da parte del personale addetto al controllo ed all’amministrazione dei profili di accesso.

Per i dati trattati su supporto cartaceo rientrano in questa categoria i rischi dovuti a :

- mancata tutela, furto, smarrimento della documentazione “in uso”; (es documentazione contenente dati sensibili, lasciata in vista di eventuali terzi non autorizzati)
- mancata tutela, furto, smarrimento della documentazione archiviata.

Per i dati trattati verbalmente rientrano in questa categoria i rischi dovuti a :

- colloqui tenuti con o in presenza di terzi non autorizzati
- richiesta e utilizzo di password altrui

#### **4.3.2 Rischi di accessi fraudolenti dall'esterno**

Per i dati trattati elettronicamente rientrano in questa categoria i rischi dovuti :

- accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software;
- “furto di identità elettronica” di un dipendente autorizzato all’accesso remoto ai sistemi;
- intercettazione di comunicazioni telematiche,
- accessi tramite collegamenti alle reti (Internet ed Intranet) da parte di operatori esterni (Hackers)

Per i dati trattati su supporto cartaceo rientrano in questa categoria i rischi dovuti a :

- mancata tutela, furto, smarrimento della documentazione “in uso”;
- mancata tutela, furto, smarrimento della documentazione archiviata.

Per i dati trattati verbalmente rientrano in questa categoria i rischi dovuti a :

- intromissione di soggetti non autorizzati in zone o locali in cui si svolgono conversazioni su informazioni riservate

#### **4.4 Disponibilità dei dati**

Il concetto di “disponibilità” si riferisce alla necessità che il sistema sia protetto da interruzioni impreviste e, conseguentemente, alla necessità che sia assicurato all’interessato il diritto di conoscere i dati personali e sanitari che possano essere trattati, nei limiti di tempo legati al raggiungimento dello scopo per cui sono stati raccolti.

I rischi di non disponibilità sono stati esaminati in relazione ad eventi di natura accidentale o intenzionale.

##### **4.4.1 Rischi di carattere accidentale**

Per i dati trattati elettronicamente sono i rischi dovuti a:

- Mancanza di alimentazione elettrica, dovuta a black-out del fornitore del servizio;
- Problemi relativi all’hw o al sw

- Errate azioni del personale incaricato che impediscono l'accesso alle informazioni

Per i dati trattati su supporto cartaceo sono i rischi dovuti a:

- irreperibilità della documentazione cartacea per perdita, furto a opera di terzi, distruzione, smarrimento
- tempi di reperimento della documentazione cartacea non congruenti con le effettive necessità di trattamento

Per i dati trattati verbalmente sono i rischi legati a:

- indisponibilità del personale che possiede l'informazione;
- carenza dei flussi informativi autorizzati

#### **4.4.2 Rischi di carattere intenzionale**

Per i dati trattati elettronicamente sono i rischi dovuti a:

- danneggiamento o manomissione volontari delle attrezzature sia hw che sw
- danneggiamento o manomissione volontari delle connessioni.

Per i dati trattati su supporto cartaceo sono i rischi di:

- furto da parte di personale interno della documentazione cartacea;
- volontario danneggiamento e/o distruzione della documentazione cartacea
- volontario occultamento della documentazione cartacea

Per i dati trattati verbalmente, sono i rischi dovuti a:

- rifiuto o reticenza nel comunicare l'informazione all'interessato a ad aventi diritto;
- generica infedeltà, o comunque negligenza del personale addetto al controllo delle informazioni.

(.....)