REGIONE AUTONOMA DELLA SARDEGNA

AZIENDA OSPEDALIERO – UNIVERSITARIA CAGLIARI
09124 Cagliari Via Ospedale 54
Telefono 070.652835 – Fax 070.6092344 info@aoucagliari.it
Partita Iva e C.F. 03108560925

Documento Programmatico sulla Sicurezza

Redatto ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003 e successive modifiche

Disposizioni minime sulla Sicurezza

Il presente documento si compone di n. 67 pagine (oltre a copertina)

Data di emissione: 24/12/2009 approvato con Delibera n. 639

Riferimenti dell'Azienda	
Sede Legale	**Via Ospedale, 54 09124 Cagliari (CA)**
Telefono	**070-51092343**
Fax	**070-51092344**
E-mail	info@aoucagliari.it
Denominazione sociale	**AZIENDA OSPEDALIERO UNIVERSITARIA**
C.F. P.IVA	**03108560925**
Rev. DPS	***1.0***

Responsabile dell'Approvazione

Nominativo	Firma
Direttore Generale Titolare del Trattamento dei dati AOU-Cagliari (Prof. Pietro Paolo Murru)	

Sommario

1.0 Introduzione 5

1.1. Campo di applicazione
1.2. Premessa 5
1.3 Definizioni 8
1.4 Riferimenti 9
1.5 Protezione dati personali 11

2.0 Principi generali per la politica della sicurezza 16

2.1 Analisi e valutazione dei rischi 17
2.2 Metodologia utilizzata per l'attuazione del piano sicurezza *19*

3.0 Politica di sicurezza 20

3.1 Ambito di attuazione del DPS 20
3.2 Standard di sicurezza 20
3.3 Organizzazione per la sicurezza 22
3.4 Classificazione della risorse 22
3.5 Sicurezza personale 22
3.6 Sicurezza materiale e ambientale 23
3.7 Gestione dei sistemi e delle reti 23
3.8 Gestione della continuità del servizio 23
3.9 Conformità 24

4.0 Natura trattamento dati afferenti AOU - Cagliari 24

5.0 Distribuzione dei compiti e delle responsabilità 26

5.1 Compiti e responsabilità 26
5.2 Il Titolare del trattamento dei dati personali. 26
5.3 Il Responsabile del trattamento dei dati personali 27
5.4 Amministratore di sistema 29
5.5 L'Incaricato del trattamento dei dati personali 29

6.0 Organigramma 30

7.0 Risorse del Sistema Informativo per il trattamento dati 30

7.1 Analisi e classificazione minacce e vulnerabilità 30

8.0 Regolamento per l'utilizzo della rete 31

8.1 Oggetto e ambito di applicazione 31
8.2 Principi generali - diritti e responsabilità 31
8.3 Abusi e attività vietate 32
8.4 Attività consentite 33
8.5 Soggetti che possono avere accesso alla rete 33
8.6 Modalità di accesso alla rete e agli applicativi 33

9.0 Video sorveglianza 34

10.0 Monitoraggio del piano 35

10.1 Monitoraggio e validazione del piano di sicurezza 35
10.2 Scheda di attuazione 35

11.0 Pianificazione degli interventi formativi 36

12.0 Evoluzione del DPS 37

Allegato 1 :Lettera di incarico ***Responsabile Trattamento Dati*** 38
Allegato 2 :Lettera di incarico ***Amministratore di sistema*** 42
Allegato 3 :Lettera di incarico ***Incaricati trattamento dati*** 43
Allegato 4 :Lettera nomina responsabile esterno ***RTI*** 45
Allegato 5 :Lettera nomina responsabile esterno ***ASL 8 - Cagliari*** 51
Allegato 6 :Lettera nomina responsabile esterno ***Ditta IMMA*** 56
Allegato 7 :Lettera informativa **dipendenti** 61
Allegato 8 :Lettera informativa **pazienti** 64

Schema 1 :***LAN AOU-Cagliari*** 67

Dichiarazione di Impegno Titolare Trattamento Dati 68

1.0 Introduzione

1.1 Campo di applicazione

La Legge n° 675/'96 sulla protezione dei dati personali, conosciuta anche come Legge sulla Privacy, ed il successivo Regolamento sulle Misure Minime di Sicurezza (D.P.R. n° 318/'99), emesso in ottemperanza all'art. 15 della citata Legge, richiedevano a tutti coloro che detenevano e trattavano dati telematici di realizzare degli specifici adempimenti formali e strutturali tesi alla loro protezione. Tali adempimenti erano denominati misure minime logiche, fisiche ed organizzative per la sicurezza dei dati. La suddetta normativa ha subito, nel corso degli ultimi anni svariate modifiche atte ad integrare e aggiornare le disposizioni emanate in materia di tutela dei dati personali. Nel Giugno 2003 è stato, infatti, emanato un nuovo Codice di protezione dei dati personali finalizzato a razionalizzare, ed a ristrutturare in parte, la normativa esistente, originando così il Decreto Legislativo 30 giugno 2003 n°196, entrato in vigore il 1° Gennaio 2004 con la denominazione sintetica di "Codice della Privacy" o più correttamente Codice in materia di protezione dei dati personali.

Il nuovo Codice della Privacy prevede l'adozione di un documento, denominato Documento Programmatico sulla Sicurezza, nel quale l'organizzazione, nella persona del titolare del trattamento dei dati, pianifica le azioni correttive e preventive (le misure di sicurezza) per contrastare le minacce che possono verificarsi sui beni informativi, sfruttando le vulnerabilità degli stessi, nonché descrive le linee guida sulle modalità di gestione dei rischi.

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato da Azienda Ospedaliero Universitaria di Cagliari, (di seguito denominata AOU – Cagliari) previsti dal D.L.vo 30/06/2003 N°. 196 "Codice in materia di protezione dei dati personali".
Il documento opportunamente integrato tiene conto del Progetto SISAR e quindi di tutti i soggetti aderenti al progetto.
Il sistema informativo descritto nel presente documento deve ritenersi sicuro in quanto strutturato secondo quanto previsto e richiesto dalla normativa per garantire la disponibilità, l'integrità e l'autenticità, nonché la riservatezza dell'informazione e dei servizi per il trattamento, attraverso l'attribuzione di specifici incarichi e le istruzioni per le persone autorizzate ad effettuare i trattamenti.

1.2 Premessa

L'Azienda Ospedaliero-Universitaria di Cagliari, istituita con deliberazione della Giunta Regionale n. 13/3 del 27 Marzo 2006 adottata in base all'art. *1 comma 3 della L.R. 28 luglio 2006 n. 10,* è operativa dal 14.05.2007 "*data di insediamento del Direttore Generale*"

L'azienda ha sede legale in Via Ospedale, 54, 09124 – Cagliari. Garantisce le prestazioni istituzionali attraverso i Presidi Ospedalieri di Monserrato del "*San Giovanni di Dio*" e le restanti strutture universitarie della "*Clinica Pediatrica*" e "*Odontoiatrica*"

Il trattamento dei dai avviene nelle seguenti Sedi:

Ospedale San Giovanni di Dio con annesso complesso Pediatrico Macciotta
Via Ospedale, 54
Cagliari

Ex Policlinico Universitario
S.S. 554 bivio per Sestu
Monserrato

Complesso Odontostomatologico
Via Binaghi
Cagliari

La Società in House SardegnaIT
Archivio dati clinici e posta certificata
c/o CRESSAN
Via Posada – Via S.Simone
Cagliari

ASL 8 Cagliari
Archivio dati previdenziali personale dipendente
Via Piero della Francesca
09047 Selargius

Salvo le sedi di Via Posada, Via S.Simone e Via Piero della Francesca, Trattasi di Ospedali e Presidi Ospedalieri articolati in strutture complesse, strutture semplici dipartimentali e strutture semplici in cui operano personale sanitario e personale amministrativo.

Sono escluse dal presente documento le Unità Operative assegnate a quest'Azienda dalla DGR 13/1 del 30.3.2007, già in regime di convenzione con la ASL 8 e ubicate presso il Presidio ospedaliero Binaghi, il Presidio ospedaliero SS. Trinità, il Presidio Ospedaliero per le Microcitemie, il Presidio Ospedaliero Marino e la Clinica psichiatrica, per le quali provvede in proprio la ASL 8 di Cagliari, con la quale persiste il regime di convenzione.

Ed inoltre i Laboratorio di Igiene degli Alimenti ed Igiene Ambientale, entrambi siti in via Porcell – Cagliari, i quali provvedono in proprio al trattamento dati.

Tipo di attività professionale esercitata

L'A.O.U.- Cagliari è la sede naturale per le attività assistenziali essenziali allo svolgimento delle funzioni istituzionali di didattica e ricerca della facoltà di medicina.

L'A.O.U.- Cagliari è una struttura di alta specializzazione .

L'A.O.U. – Cagliari ha come scopo il perseguimento del più alto livello di assistenza a fronte dei bisogni della popolazione in un processo che include:

- didattica, quale strumento di miglioramento continuo delle competenze di tutti gli operatori e dei soggetti in formazione;;

- ricerca, rivolta all'innovazione e sviluppo delle procedure diagnostiche-cliniche delle conoscenze biomediche e tecnologiche;

L'A.O.U.- Cagliari svolge la propria attività mediante un processo di programmazione aziendale sulla base degli indirizzi di pertinenza della Regione – Università - Facoltà di Medicina, nell'ambito

delle risorse disponibili, che verranno utilizzate secondo criteri di efficienza, efficacia ed economicità.

L'azienda, quale componente di un sistema integrato, sviluppa la cooperazione fra le diverse Aziende Sanitarie per garantire l'uniformità e l'unitarietà delle funzioni del S.S.R., per garantire omogeneità, aldilà della loro differenza, all'organizzazione e funzionamento delle Aziende Sanitarie per facilitare la mobilità degli operatori e le politiche del personale, per agevolare i rapporti con i soggetti istituzionali e con i cittadini.

Il principale scopo del presente DPS è dunque di illustrare:

- il quadro normativo di riferimento;
- il quadro metodologico di riferimento per la gestione della sicurezza nel trattamento dei dati:
  - ambito di applicazione del DPS
  - Attuazione del DPS
  - Politiche di sicurezza
- La struttura della AOU - Cagliari e l'organizzazione per la sicurezza nel trattamento dei dati;
- le procedure di lavoro e gli asset informativi (beni informativi)
- la classificazione delle minacce e delle vulnerabilità per l'analisi dei rischi;
- le tecniche di monitoraggio dell'attuazione del DPS;
- le tecniche di manutenzione ed evoluzione del DPS;

Il campo di applicazione dei precedenti argomenti è esteso a tutte le procedure operative della AOU - Cagliari nell'ambito dei trattamenti dei dati personali.

Il presente documento descrive un piano per la sicurezza che garantisce, per ogni dato personale:

- la riservatezza delle informazioni,
- l'integrità delle informazioni,
- la disponibilità delle informazioni,
- la continuità delle attività legate ai processi,

Per raggiungere gli scopi precedentemente descritti, nel presente documento è stata individuata la seguente classificazione degli asset:

- Informazioni (cartacee ed elettroniche a trattamento informatico)
- Reti
- Infrastrutture
- Hardware
- Software
- Risorse umane.

Tutti gli asset sono quindi ricondotti ad elementi di questa classificazione. Si fa rilevare, inoltre, che, nel seguito, per ogni attività, sono stati elencati un insieme di controlli da attuare incondizionatamente per garantire livelli minimi per la protezione degli asset individuati.

Il presente documento è stato elaborato in coerenza con:

- le linee guida emanate in materia dagli organismi tecnici di standardizzazione internazionale;
- gli orientamenti tecnici indicati dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione);
- le raccomandazioni del Garante della Privacy in materia di attuazione del decreto sulla protezione dei dati personali nell'ambito sanitario, specificatamente quello pubblico.

1.3 DEFINIZIONI

Ai fini del presente documento si intende per:

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

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

dati identificativi
i dati personali che permettono l'identificazione diretta dell'interessato;

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

dati giudiziari
dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

comunicazione
il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

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

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

blocco
la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento

banca di dati
qualsiasi complesso organizzato di dati personali, ripartiti in una o più unità dislocate in uno o più siti;
Garante della privacy
l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
interessato
Proprietario dei dati personali di cui si effettua un trattamento;
informazione
Dato o dati conservati o processati nei sistemi o su dispositivi rimovibili durante l'esecuzione di processi organizzativi;
sicurezza
Protezione dell'informazione dalla distruzione, dalle modifiche e dalla divulgazione non autorizzate;
riservatezza
Protezione contro la divulgazione di informazioni senza il consenso dell'interessato;
integrità
Protezione contro la modifica, la creazione o la replica non autorizzata delle informazioni;
disponibilità
Protezione contro ritardi non accettabili nell'accesso autorizzato alle informazioni;
autenticità
Principio che assicura che un'informazione sia stata fornita da chi sostiene essere l'autore e non è stata alterata in nessun modo da una terza parte;
responsabilità
Principio che garantisce l'imputabilità ad ogni soggetto degli effetti di ciascuna azione dal medesimo compiuta;
asset
Qualunque tipo di risorsa utile al trattamento dei dati personali, anche mediante un processo complesso;
affidabilità
Principio che indica la capacità di un asset di sopportare senza danni irreparabili, l'impatto di eventi imprevisti.

1.4 Riferimenti

- Carta dei Servizi – Organizzazione e Funzionamento dell'Azienda AOU - Cagliari.
- Decreto del Presidente della Giunta Regionale n. 1394/1 del 9 luglio 2003,nomina Sardegna IT s.r.l., società "in house" della Regione Sardegna Responsabile del. trattamento dei dati personali "per tutti i progetti informatici ad essa affidati";
- Delibera della Giunta Regionale N. 32/4 del 13/07/2005 "Piano per l'informatizzazione del Sistema Sanitario Regionale", che prevede: "un centro regionale per i servizi sanitari (CRESSAN);
- atto del 29.05.2006 della Regione Autonoma della Sardegna - Direzione generale della sanità - Servizio Affari generali ed istituzionali e sistema informativo, affidamento a Sardegna IT l'attuazione dell'intervento "Costituzione, avviamento e messa in funzione del CRESSAN - Centro Regionale dei Servizi informatici e telematici per il sistema Sanitario"
- allegato A all'atto di affidamento del 29.05.2008 punto 1.06 la "Gestione servizi di posta elettronica e posta elettronica certificata per il sistema regionale sanitario" ;
- Codice di deontologia medica.

- Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alla distribuzione delle funzioni di amministratore di sistema 27 Novembre 2008 – G.U n°300 24/12/2008
- Autorizzazione n. 2/2008 al trattamento dei dati idonei a rilevare lo stato di salute e la vita sessuale 19 giugno 2008 G.U. del 21.7.2008 suppl. Ord. N.175
- Parere dell'Autorità Garante del 13 aprile 2006: Trattamento dei dati sensibili e giudiziari da effettuarsi presso le regioni, le province autonome e le aziende sanitarie.
- Direttiva del Garante- Strutture sanitarie: rispetto della dignità - 9 novembre 2005.
- Regolamento Garante sulla videosorveglianza. - 29 aprile 2004
- D.M. 26 luglio 1993 (G.U. 3 agosto 1993, n. 180). "Disciplina del flusso informativo sui dimessi dagli istituti di ricovero pubblici e privati"
- Articoli 622 e 326 del Codice Penale (Il segreto professionale, assoluto e inderogabile nella sua sacralità già nel Giuramento di Ippocrate, rappresenta un fondamentale obbligo sia etico che giuridico: la violazione del segreto professionale è penalmente sanzionata. In particolare «i medici non possono fornire alcuna indicazione sulle condizioni di un paziente, nemmeno ai parenti più prossimi senza il consenso dell'interessato».
- Art. 734 bis codice penale-Divulgazione delle generalità o dell'immagine di persona offesa da atti di violenza sessuale."Chiunque, nei casi di delitti previsti dagli articoli 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-ter, 609-quater, 609-quinquies e 609-octies, divulghi, anche attraverso mezzi di comunicazione di massa, le generalità o l'immagine della persona offesa senza il suo consenso, è punito con l'arresto da tre a sei mesi."
- Art. 11 L. 22 maggio 1978 n. 194 Norma per la tutela sociale della maternità e sull'interruzione volontaria della gravidanza prevedendo che l'ente che effettua l'operazione protegge l'identità della donna.
- Art. 5 legge 5 giugno 1990 n. 135. 1. Gli operatori sanitari che, nell'esercizio della loro professione, vengano a conoscenza di un caso di AIDS, ovvero di un caso di infezione da HIV, anche non accompagnato da stato morboso, sono tenuti a prestare la necessaria assistenza adottando tutte le misure occorrenti per la tutela della riservatezza della persona assistita. 2. Fatto salvo il vigente sistema di sorveglianza epidemiologica nazionale dei casi di AIDS conclamato e le garanzie ivi previste, la rilevazione statistica della infezione da HIV deve essere comunque effettuata con modalità che non consentano l'identificazione della persona. La disciplina per le rilevazioni epidemiologiche e statistiche è emanata con decreto del Ministro della sanità che dovrà prevedere modalità differenziate per i casi di AIDS e i casi di sieropositività. 3. Nessuno può essere sottoposto, senza il suo consenso, ad analisi tendenti ad accertare l'infezione da HIV se non per motivi di necessità clinica nel suo interesse. Sono consentite analisi di accertamento di infezione da HIV, nell'ambito di programmi epidemiologici, soltanto quando i campioni da analizzare siano stati resi anonimi con assoluta impossibilità di pervenire alla identificazione delle persone interessate. 4. La comunicazione di risultati di accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti. 5. L'accertata infezione da HIV non può costituire motivo di discriminazione, in particolare per l'iscrizione alla scuola, per lo svolgimento di attività sportive, per l'accesso o il mantenimento di posti di lavoro.
- Per quanto riguarda i problemi connessi alla cartella clinica con particolare riferimento alla regolare compilazione, al segreto, alla conservazione e alla circolazione nonché alla modalità del suo rilascio, tutte attività che incidono particolarmente sulla privacy del paziente, i riferimenti normativi sono i seguenti: COMPILAZIONE: R.D. 30 settembre 1938

numero 1631 art. 24 - D.P.R. 27 marzo 1969 numero 128 art. 2 7 -D.P.R. 14 marzo 1974 numero 225 (abrogato dalla legge 42/99) -Codice di deontologia medica - CONSERVAZIONE: Costituzione italiana art. 97-D.P.R. 27 marzo 1969 numero 128 art. 7-D.P.R. 14 marzo 1974 numero 225-D.P.R. 27 marzo 1969 numero 128 art. 2 – 5- codice di deontologia medica -Circolare Ministero della sanità 19 dicembre 1986- E' prevista la possibilità della microfilmatura: legge 4 gennaio 1968 numero 15 - -D.P.R. 28 dicembre 2000 numero 445- CIRCOLAZIONE- D.P.R. 27 marzo 1969 numero 128 art. 5- codice di deontologia - Parere dell'Autority per la privacy 19 maggio 2000-DLgs 30 luglio 1999 numero 282 registrazione in cartella dei test genetici. Nel corso dell'anno successivo saranno ulteriormente analizzate tali argomentazioni.

- Provvedimento del 27.11.08 del garante per la protezione dei dati personali in punto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"
  Disposizione del 12.2.09 del garante in tema di Unificazione e proroga dei termini per l'adempimento delle prescrizioni impartite con il provvedimento del 27.11.2008 ai titolari del trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.

1.5 Protezione dati personali

Il DPS rappresenta una misura minima di sicurezza che raggruppa altre misure di prevenzione e protezione dei dati personali e degli asset utilizzati.

In tale contesto, la normativa in esame impone *di "ridurre al minimo", mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta" (art. 31): identificando le risorse da proteggere; operando una opportuna e attenta analisi dei rischi; programmando un adeguamento progressivo; adottando le misure di sicurezza obbligatorie (fisiche, logiche ed organizzative); adeguandosi agli obblighi di informativa, consenso, notifica, nomina delle figure professionali (responsabili, incaricati, custode delle credenziali ecc.); redigendo un apposito "Documento Programmatico sulla Sicurezza" da aggiornare annualmente entro il 31/3.*

La gestione del DPS deve evolversi con l'organizzazione per il trattamento dei dati e deve includere:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati;
- i criteri e le modalità di ripristino dell'accesso ai dati, in seguito a distruzione o danneggiamento degli stessi o degli strumenti elettronici;
- la previsione di interventi formativi degli incaricati al trattamento;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

La normativa sancisce i principi di tutela dei dati personali:

- liceità di raccolta e trattamento dei dati
- uso per scopi legittimi e determinati
- uso non diverso da quanto dichiarato
- adeguati pertinenti e non eccedenti
- esatti e aggiornati
- conservati solo per il tempo necessario
- garantiti nella sicurezza e nell'accesso

a) autenticazione informatica ed adozione di procedure di gestione delle credenziali di autenticazione:
   - si tratta di verificare l'identità di chi andrà a trattare i dati e convalidarla dopo averla verificata

b) utilizzazione di un sistema di autorizzazione:
   - successivamente all'autenticazione informatica del soggetto, altri strumenti e procedure (sistema di autorizzazione) permetteranno al soggetto identificato e autenticato di accedere ai trattamenti dei dati ai quali è stato preventivamente autorizzato.
     E' prevista la possibilità di utilizzo della scheda CNS
     La Carta Nazionale dei Servizi (CNS) è un documento informatico, rilasciato da una Pubblica Amministrazione, con la finalità di identificare in rete il titolare della carta.
     Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete.
     Ogni CNS contiene i dati identificativi della persona e il codice fiscale, il certificato di autenticazione che, in combinazione con il PIN fornito dall'Ente emettitore consente l'autenticazione in rete, e può contenere anche il certificato di firma digitale

c) aggiornamento periodico della individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici:
   - profili di autorizzazione
   - autorizzati per iscritto
   - sottoposti a verifica almeno una volta all'anno

d) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici:
   - protezione dalle azioni distruttive di virus, worm, codice maligno e pericoloso per l'integrità, la confidenzialità e la disponibilità degli stessi
   - adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.
   - copie di sicurezza (backup)
   - recupero di dati danneggiati o persi (restore)

La validità di tali misure di sicurezza è garantita dal monitoraggio sullo stato di efficienza ed efficacia della loro applicazione nonché dalla loro programmaticità e revisionabilità, sia nei casi privi di problematiche, sia all'occorrenza, per rimediare immediatamente ad eventuali, impreviste e nuove minacce. Il piano della sicurezza, quindi, sarà aggiornato con una nuova analisi dei rischi ogniqualvolta si verifichino circostanze che possano comprometterne la validità e l'efficacia.

Il Garante, inoltre, il 9 novembre 2005 ha prescritto a tutti i titolari del trattamento di dati personali interessati in ambito sanitario, ai sensi dell'art. 154, comma 1, lett. c), del Codice di adottare, ove già non attuate, le misure necessarie od opportune al fine di rendere il trattamento dei medesimi dati conforme alle disposizioni vigenti, sulla base dei principi richiamati dal provvedimento e dei chiarimenti con esso forniti; ha prescritto ai medesimi titolari, ai sensi dell'art. 154, comma 1, lett. c), del Codice di adottare comunque tutte le ulteriori misure per garantire, in materia di trattamento dei dati personali nell'ambito sanitario, il massimo rispetto del principio di dignità. In particolare è tutelata:

La dignità dell'interessato
La prestazione medica e ogni operazione di trattamento dei dati personali deve avvenire nel pieno rispetto della dignità dell'interessato

La tutela della dignità personale deve essere garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria, con particolare riguardo a fasce deboli quali i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno.

Particolare riguardo deve essere prestato nel rispettare la dignità di pazienti sottoposti a trattamenti medici invasivi o nei cui confronti è comunque doverosa una particolare attenzione anche per effetto di specifici obblighi di legge o di regolamento o della normativa comunitaria (ad es., in riferimento a sieropositivi o affetti da infezione da Hiv –l. 5 giugno 1990, n. 135-, all'interruzione di gravidanza – l. 22 maggio 1978, n. 194- o a persone offese da atti di violenza sessuale -art. 734-bis del codice penale-).

La necessità di rispettare la dignità è stata rappresentata a questa Autorità anche in relazione alle modalità di visita e di intervento sanitario effettuati nelle aziende ospedaliero-universitarie alla presenza di studenti autorizzati. Le strutture che intendono avvalersi di questa modalità devono indicare nell'informativa da fornire al paziente che (*art. 13 del Codice*), in occasione di alcune prestazioni sanitarie, si perseguono anche finalità didattiche, oltre che di cura e prevenzione (*cfr. d.lg. n. 517/1999*). Durante tali prestazioni devono essere adottate specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie

La riservatezza nei colloqui e nelle prestazioni sanitarie.
É doveroso adottare idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate.

Il rispetto di questa garanzia non ostacola la possibilità di utilizzare determinate aree per più prestazioni contemporanee, quando tale modalità risponde all'esigenza terapeutica di diminuire l'impatto psicologico dell'intervento medico (ad es., alcuni trattamenti sanitari effettuati nei confronti di minori).

Le notizie su prestazioni di pronto soccorso
L'organismo sanitario può dare notizia, anche per via telefonica, circa una prestazione di pronto soccorso, ovvero darne conferma a seguito di richiesta anche per via telefonica.

La notizia o la conferma devono essere però fornite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso.

Questo genere di informazioni riguarda solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso, e non attiene ad informazioni più dettagliate sullo stato di salute.

L'interessato -se cosciente e capace- deve essere preventivamente informato dall'organismo sanitario (ad es. in fase di accettazione), e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

Il personale incaricato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall'interessato.

La dislocazione dei pazienti nei reparti
Il Codice incentiva le strutture sanitarie a prevedere, in conformità agli ordinamenti interni, le modalità per fornire informazioni ai terzi legittimati circa la dislocazione dei degenti nei reparti, allorché si debba ad esempio rispondere a richieste di familiari e parenti, conoscenti e personale del volontariato.

L'interessato cosciente e capace deve essere, anche in questo caso, informato e posto in condizione (ad es. all'atto del ricovero) di fornire indicazioni circa i soggetti che possono venire a conoscenza del ricovero e del reparto di degenza. Occorre altresì rispettare l'eventuale sua richiesta che la presenza nella struttura sanitaria non sia resa nota neanche ai terzi legittimati .Come per le prestazioni di pronto soccorso, questo genere di informazioni riguarda la sola presenza nel reparto e non anche informazioni sullo stato di salute.

Possono essere fornite informazioni sullo stato di salute a soggetti diversi dall'interessato quando sia stato manifestato un consenso specifico e distinto al riguardo, consenso che può essere anche manifestato da parte di un altro soggetto legittimato, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato

La distanza di cortesia.
Le strutture sanitarie devono predisporre apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento di dati sanitari (es. operazioni di sportello, acquisizione di informazioni sullo stato di salute), nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato.

Vanno in questa prospettiva prefigurate appropriate soluzioni, sensibilizzando gli utenti con idonei inviti, segnali o cartelli.

L' ordine di precedenza e di chiamata.
All'interno dei locali di strutture sanitarie, nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa (ad es., in caso di analisi cliniche), devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli interessati che prescinda dalla loro individuazione nominativa (ad es., attribuendo loro un codice

numerico o alfanumerico fornito al momento della prenotazione o dell'accettazione). Ovviamente, tale misura non deve essere applicata durante i colloqui tra l'interessato e il personale medico o amministrativo.

Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'interessato (ad es. in funzione di particolari caratteristiche del paziente anche legate ad uno stato di disabilità), possono essere utilizzati altri accorgimenti adeguati ed equivalenti (ad es., con un contatto diretto con il paziente).

Non risulta giustificata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di intervento effettuato o ancora da erogare (es. liste di degenti che devono subire un intervento operatorio). Non devono essere, parimenti, resi facilmente visibili da terzi non legittimati i documenti riepilogativi di condizioni cliniche dell'interessato (es. cartelle infermieristiche poste in prossimità del letto di degenza) .

La correlazione fra paziente e reparto o struttura.

Gli organismi sanitari devono mettere in atto specifiche procedure, anche di formazione del personale, per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si è recato o è stato ricoverato.

Tali cautele devono essere orientate anche alle eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura (ad es., per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale).

Analoghe garanzie devono essere adottate da tutti i titolari del trattamento, ivi comprese le farmacie, affinché nella spedizione di prodotti non siano indicati, sulla parte esterna del plico postale, informazioni idonee a rivelare l'esistenza di uno stato di salute dell'interessato (ad es., indicazione della tipologia del contenuto del plico o del reparto dell'organismo sanitario mittente).

Per quanto riguarda **le regole di condotta per gli incaricati,** si stabilisce che il titolare del trattamento deve designare quali incaricati o, eventualmente, responsabili del trattamento i soggetti che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi per svolgere le attività di prevenzione, diagnosi, cura e riabilitazione, nonché quelle amministrative correlate .

Fermi restando, in quanto applicabili, gli obblighi in materia di segreto d'ufficio, deve essere previsto che, al pari del personale medico ed infermieristico, già tenuto al segreto professionale (*codice di deontologia codice deontologico per gli infermieri*), gli altri soggetti che non sono tenuti per legge al segreto professionale (ad es., personale tecnico e ausiliario) siano sottoposti a regole di condotta analoghe.

A tal fine, anche avvalendosi di iniziative di formazione del personale designato, occorre mettere in luce gli obblighi previsti dalla disciplina in materia di protezione dei dati personali con particolare riferimento all'adozione delle predette misure organizzative , evidenziando i rischi, soprattutto di accesso non autorizzato, che incombono sui dati idonei a rivelare lo stato di salute e le misure disponibili per prevenire effetti dannosi.

Comunicazione di dati all'interessato

Gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni sul suo stato di salute solo per il tramite di un medico (individuato dallo stesso interessato, oppure dal titolare del trattamento) o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente (ad es., un infermiere designato quale incaricato del trattamento ed autorizzato per iscritto dal titolare).
La necessità di rispettare queste modalità andrebbe menzionata nelle istruzioni impartite agli incaricati del trattamento . Nel caso in cui l'interessato riceva una comunicazione dalla struttura sanitaria che documenti gli esiti di esami clinici effettuati, l'intermediazione può essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta.

Il personale designato deve essere istruito debitamente anche in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'interessato (es. referti diagnostici). In riferimento alle numerose segnalazioni pervenute, va rilevato che le certificazioni rilasciate dai laboratori di analisi o dagli altri organismi sanitari possono essere ritirate anche da persone diverse dai diretti interessati, purché sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa."

2.0 Principi generali per la politica della sicurezza

Le norme che prescrivono le misure di sicurezza appaiono, così, soprattutto come lo sviluppo minimo di tre principi che sono alla base degli standard, delle raccomandazioni e delle linee guida per la sicurezza:

- **integrità**: intesa come la gestione dell'accuratezza e completezza delle informazioni e delle relative applicazioni, la salvaguardia della accuratezza e completezza dei dati, la difesa da manomissioni o modifiche non autorizzate;
- **confidenzialità**/**riservatezza**: intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate, la protezione delle trasmissioni, il controllo degli accessi;
- **disponibilità**: intesa come l'assicurazione che l'accesso ai dati sia disponibile quando occorre ed in un contesto pertinente, quindi la garanzia per gli utenti della fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi.

In un sistema informatico, si ha piena disponibilità dei dati se questi possono essere trattati direttamente dagli utenti che ne hanno facoltà perché ne sono autorizzati, o, indirettamente, dai processi di elaborazione lecita, nel momento in cui essi servono o sono richiesti secondo modalità e tempi prestabiliti. Estendendo una siffatta definizione nella generalità, un sistema informatico che goda della proprietà della disponibilità è un sistema che garantisce la funzionalità anche in situazioni critiche, come nei casi di avarie, con fattori tecnici di qualità, quali, la robustezza del sistema e la tolleranza ai guasti che assicurano il recupero di dati e situazioni di blocco operativo. Sistemi con tali funzionalità forniscono un elevatissimo livello di disponibilità dell'informazione.

A questo punto appare evidente che un sistema che sia "disponibile", nel senso che rende possibile il trattamento delle informazioni in ogni evenienza, è un sistema che garantisce la continuità funzionale o di servizio. Per molte organizzazioni, come quelle appartenenti al comparto della

Sanità ed alla Pubblica Amministrazione o le aziende che erogano servizi per esse, la continuità del servizio è una prerogativa fondamentale per stabilire un corretto rapporto con i propri utenti e mira ad innalzare il grado di soddisfazione dell'utenza che fruisce dei servizi erogati, oltre che a migliorare il livello di gestione delle procedure interne. In altri termini, la continuità del servizio è un obiettivo fondamentale del DPS.

La riservatezza è l'altro paradigma informatico a cui si è accennato in precedenza. Questo concetto è apparentemente più intuitivo da comprendere, in quanto si riferisce alla sfera di riserbo con la quale bisogna trattare i dati.
Nel caso dei sistemi informatici, è evidente che la riservatezza viene violata quando il sistema in questione non è in grado di impedire, a chiunque non sia autorizzato, di conoscere informazioni.

Naturalmente, quando si parla di sistema, bisogna riferirsi non solo alle caratteristiche intrinseche dell'hardware e del software, ma anche all'organizzazione delle risorse umane e del sistema informatico nonché alle modalità con le quali sono predisposti i componenti utilizzabili dagli utenti.

In altre parole, con il presente DPS si è definito un "Progetto per la Sicurezza",
La sicurezza informatica, in particolare, si ottiene implementando una serie di controlli che analizzano e controllano le politiche di gestione, le regole di corretto utilizzo, le procedure, le infrastrutture organizzative e le misure tecnologiche. Tali controlli hanno l'obiettivo di garantire che i requisiti di sicurezza stabiliti dall'organizzazione siano soddisfatti con continuità.

2.1 Analisi e valutazione dei rischi

Per l'organizzazione dell'azienda sanitaria dunque è essenziale riuscire a definire i propri obiettivi di sicurezza. I principali fattori da valutare per definire l'adeguato livello di sicurezza sulle risorse ritenute importanti o sensibili sono:

- **analisi del rischio**: essa consente di identificare le possibili minacce con la relativa probabilità di occorrenza e di valutare il livello di vulnerabilità ed il potenziale impatto, in termini di danni, sulle risorse da proteggere;
- **valutazione dei vincoli legali, di statuto e contrattuali** che l'organizzazione deve rispettare nei confronti di terze parti, siano essi partner, fornitori di servizi, ecc.;
- **valutazione dell'insieme di principi**, regole ed obiettivi relativi alla gestione dell'informazione che l'organizzazione ha sviluppato al fine di supportare i propri flussi operativi.

L'analisi dei rischi effettuata passa attraverso le seguenti fondamentali valutazioni:

- valutazione delle debolezze presenti nelle strutture fisiche
- valutazione delle minacce presenti e/o probabili negli elaboratori
- valutazione delle minacce presenti e/o probabili sui dati e sul software
- valutazione delle minacce presenti e/o probabili sulle strutture di rete
- valutazione delle minacce presenti e/o probabili sugli accessi telematici
- valutazione delle minacce presenti e/o probabili sugli operatori

La metodologia messa in atto per l'analisi dei rischi, è tale che induce a valutare anche le dipendenze e le correlazioni che possono innestarsi tra gli stessi eventi.

Infine, la misura del rischio può essere calcolata attraverso una tabella di correlazione che consente di rilevare, per ogni minaccia possibile, le criticità relative alle singole risorse.

L'analisi di tale tabella permette di capire quali sono i principali problemi, in termini di minacce e vulnerabilità, che minano la sicurezza.

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse.

Rischi	Deliberato	Accidentale	Ambientale	Livello
Terremoto			X	basso
Inondazione	X	X	X	basso
Uragano			X	basso
Fulmine			X	basso
Bombardamento	X	X		basso
Fuoco	X	X		medio
Uso di armi		X		medio
Danno volontario	X			medio
Interruzione di corrente		X		medio
Interruzione di acqua		X		medio
Interruzione di aria condizionata	X	X		medio
Guasto hardware		X		medio
Linea elettrica instabile		X	X	medio
Temperatura e umidità eccessive			X	alto
Polvere			X	basso
Radiazioni elettromagnetiche		X		basso
Scariche elettrostatiche		X		basso
Furto	X			medio
Uso non autorizzato dei supporti di memoria	X			basso
Deterioramento dei supporti di memoria		X		basso
Errore del personale operativo		X		basso
Errore di manutenzione		X		basso
Masquerading dell'identificativo dell'utente	X			basso
Uso illegale di software	X	X		basso
Software dannoso		X		basso
Esportazione/importazione illegale di software	X			basso

Rischi	Deliberato	Accidentale	Ambientale	Livello
Accesso non autorizzato alla rete	X			basso
Uso della rete in modo non autorizzato	X			basso
Guasto tecnico di provider di rete		X		basso
Danni sulle linee	X	X		basso
Errore di trasmissione		X		basso
Sovraccarico di traffico	X	X		basso
Intercettazione (Eavesdropping)	X			basso
Infiltrazione nelle comunicazioni	X			basso
Analisi del traffico		X		basso
Indirizzamento non corretto dei messaggi		X		basso
Reindirizzamento dei messaggi	X			basso
Ripudio	X			basso
Guasto dei servizi di comunicazione	X	X		basso
Mancanza di personale		X		basso
Errore dell'utente	X	X		basso
Uso non corretto delle risorse	X	X		basso
Guasto software	X	X		basso
Uso di software da parte di utenti non autorizzati	X	X		basso
Uso di software in situazioni non autorizzate	X	X		basso

2.2 *La metodologia utilizzata per l'attuazione del piano sicurezza*

Un corretto approccio alle problematiche della sicurezza richiede di considerare contemporaneamente gli aspetti Ambientali (sicurezza fisica), Tecnici (sicurezza fisica e logica), Organizzativi (definizione di ruoli, procedure, formazione), Economici (analisi dei costi) ed infine Legali (leggi e raccomandazioni, normative).
Per la gestione organizzativa e procedurale della sicurezza informatica si fa riferimento alle norme standard BS7799 che indirizzano in modo specifico i temi della sicurezza nei seguenti capitoli:

1. Politiche della sicurezza
2. Sicurezza organizzativa
3. Classificazione e controllo degli asset
4. Sicurezza del personale
5. Sicurezza fisica ed ambientale
6. Operazioni e comunicazioni
7. Controllo accessi
8. Sviluppo e manutenzione
9. Business continuity
10. Conformità.

Per la corretta applicazione delle norme BS7799 è necessario predisporre ed attuare adeguati strumenti e controlli per la gestione e il monitoraggio della sicurezza. Tali controlli devono essere realizzati attraverso:

- meccanismi hardware o software (sistemi di autenticazione tramite password, token card, smart card, prodotti per la protezione crittografica dei dati, firewall, etc.);
- sistemi anti intrusione, telecamere, casseforti, contenitori ignifughi, etc.;
- la creazione di apposite strutture o funzioni all'interno dell'organizzazione e la definizione di procedure organizzative (ad esempio l'istituzione di un forum per la gestione della sicurezza dell'informazione, l'affidamento dell'incarico di formazione periodica del personale, le procedure per l'accettazione di ospiti all'interno dell'organizzazione, ecc.).

L'applicazione della metodologia BS7799 si articola nelle seguenti fasi principali:

- analisi conoscitiva dell'organizzazione,
- politiche generali di sicurezza delle informazioni,
- analisi e gestione del rischio.

Le politiche della sicurezza saranno sottoposte a revisione periodica affinché rimangano appropriate ai cambiamenti interni ed esterni.

3.0 Politica di sicurezza

3.1 *Ambito di attuazione del DPS*

L'ambito cui si applicano tutti i criteri e le procedure descritte nel presente DPS è quello relativo a: le procedure operative della AOU – Cagliari nell'ambito dei trattamenti dei dati personali,

Tali procedure riguardano tutte le strutture in cui l'organizzazione è suddivisa e le seguenti tipologie di dati:

- personali
- identificativi
- sensibili
- giudiziari
- particolari

nonché le risorse necessarie al loro trattamento.

3.2 *Standard di sicurezza*

L'obiettivo è quello di dare direttive per la gestione delle informazioni di sicurezza.

Principi generali:

1. il trattamento dei dati personali attraverso l'uso dei beni informativi di proprietà della AOU - Cagliari deve avvenire nel rispetto dei principi di riservatezza stabiliti dal d.lgs. 196/2003 e dai contratti in vigore;

2. tutti gli accessi agli archivi cartacei, ai data-base, al software ed ai servizi applicativi, alle strumentazioni elettroniche ed ai locali dove si svolgono i trattamenti dei dati, deve avvenire tramite un sistema di autenticazione ed autorizzazione, di tipo fisico, logico od organizzativo. In particolare per sistema fisico, si intende l'accesso ai locali e suppellettili di ufficio consentito a seguito dell'incarico al trattamento dei dati al personale o altre persone fisiche o giuridiche individuate dal responsabile del trattamento stesso; per sistema logico, si intende il meccanismo software (user id e password) per l'accesso a data-base, elenchi elettronici di dati personali, software, servizi applicativi, reti e domini telematici; per sistema organizzativo, si intende l'insieme delle misure che impattano sull'organizzazione, quale la formazione, l'attribuzione di responsabilità, la delimitazione di ambiti di trattamento, e considerate idonee per consentire l'uso consapevole e responsabile dei beni informativi;
3. tutte le informazioni (dati, documenti, archivi, …) devono essere protette, aggiornate, corrette, rese disponibili ed integre ai soggetti autorizzati al trattamento;
4. per la riservatezza delle informazioni scambiate internamente o con l'esterno, la sicurezza deve essere garantita anche a livello delle reti di comunicazioni dati;
5. tutte le misure adottate devono essere oggetto di monitoraggio costante;
6. devono essere predisposte adeguate misure di sicurezza per l'accesso ai locali dove si svolgono i trattamenti, anche quando i locali sono ubicati all'esterno presso terzi, e per la protezione del materiale utile ai trattamenti, le infrastrutture tecnologiche ed ambientali (sistemi di condizionamento, sistemi allarme, sistemi anti-incendio, apparati elettrici, ecc.);
7. ogni eventuale incidente o evento straordinario che possa pregiudicare la sicurezza deve essere oggetto di analisi e di rapporto scritto;
8. tutte le postazioni di lavoro devono essere utilizzate solo per i trattamenti consentiti e non eccedenti le operazioni da svolgere;
9. devono essere utilizzati solo software autorizzati dal Titolare e/o dai Responsabili;
10. tutti i progetti di nuove applicazioni/servizi devono essere inseriti nel piano per la sicurezza del DPS;
11. tutte le modifiche, eventualmente apportate ai processi organizzativi interni devono essere inserite nel DPS;
12. nel caso in cui si dovessero utilizzare eventuali centri esterni di trattamento dei dati, devono essere gestiti in sicurezza tutti i possibili trasferimenti di informazioni e altri beni informativi, in generale, e, in particolare, bisogna porre la massima cautela nel trattare tutte le componenti e le informazioni sensibili;
13. i servizi di monitoraggio degli accessi devono essere estesi a tutti gli apparati di elaborazione elettronica dei dati. In particolare, per fini di controllo e sicurezza, i sistemi di elaborazione dovranno consentire la gestione dei file di log, quando le tecnologie software utilizzate lo permettono:
    - identificazione di ogni nodo di rete;
    - tracciatura ed identificazione delle operazioni;
14. relativamente alle problematiche di sicurezza inerenti l'evasione di richieste di trattamenti eccedenti la gestione ordinaria dei dati effettuata da parte del personale della AOU-Cagliari

o da parte di altri soggetti, tali richieste dovranno essere sempre autorizzate per iscritto dal titolare.

3.3 *Organizzazione per la sicurezza*

La AOU - Cagliari definisce le responsabilità per il trattamento dei dati, assegnandole formalmente ai soggetti individuati, aggiorna tali attribuzioni, in funzione degli ambiti di trattamento, delle variazioni organizzative, delle necessità variate per l'introduzione di nuovi sistemi di elaborazione e trasmissione delle informazioni.
Inoltre, costituisce un gruppo di lavoro per la gestione della problematica della privacy e della sua applicazione. Tale gruppo coadiuva i Responsabili del trattamento dei dati per l'attuazione delle prescrizioni normative.
I Responsabili del trattamento dei dati individuano le necessità di formazione sia per l'aggiornamento continuo del personale, sia in occasione di nuove assunzioni o modifiche di mansioni o ruoli interni da parte del personale stesso.

3.4 Classificazione e Controllo delle risorse

Vengono raccolte e classificate informazioni relative ai beni informativi. In particolare le risorse da considerare sono:

- Persone assunte, collaboratori e consulenti, soggetti giuridici esterni
- Basi-dati
- Documentazioni cartacee di varia natura
- Elenchi di dati di persone fisiche e giuridiche
- Sistemi informativi e software
- Sistemi ed apparati di rete tra le varie sedi (intranet, internet)
- Sistemi Server
- Postazioni di lavoro
- Domini di reti e servizi applicativi
- Sito internet
- Locali ed ambienti
- Sistemi di conservazione
- Supporti elettronici per la memorizzazione di dati

Tutte le risorse individuate devono rientrare nelle seguenti classi di Asset:

- Informazioni (cartacee ed elettroniche a trattamento informatico)
- Reti
- Infrastrutture
- Hardware
- Software
- Risorse umane.

3.5 Sicurezza del personale

Gli obiettivi di questa linea guida sono:

- ridurre il rischio di errori umani, furto, frode o uso improprio delle strutture aziendali;

- accertarsi che il personale addetto sia stato informato sui possibili rischi relativi alla sicurezza delle informazioni.

3.6 Sicurezza materiale e ambientale

Gli obiettivi di questa linea guida sono:

- impedire l'accesso non autorizzato, il danneggiamento e l'interferenza all'interno del flusso delle informazioni;
- impedire la perdita o il danneggiamento dei dati necessari alla corretta esecuzione dei processi operativi
- impedire l'interruzione delle attività

3.7 Gestione dei sistemi e delle reti

Gli obiettivi di questa linea guida sono:

- assicurare il corretto e sicuro funzionamento sistemi di elaborazione e delle reti;
- minimizzare il rischio di guasti dei sistemi;
- proteggere l'integrità del software di base e delle informazioni;
- assicurare la disponibilità dei processi di elaborazione dell'informazione e di comunicazione;
- garantire la salvaguardia delle informazioni in rete e la protezione delle infrastrutture di rete;
- evitare la perdita, modifica o uso improprio delle informazioni scambiate in rete.

3.8 Gestione della continuità del servizio

Per una corretta gestione del governo delle informazioni i sistemi devono garantire la continuità dei servizi.

Di seguito è sintetizzata una classificazione di eventi straordinari:

- Un disastro di primo livello su un ufficio può causare, in alcuni casi, la parziale ma non completa distruzione delle operazioni svolte giornalmente. La situazione può essere risolta usando personale dell'ufficio stesso ed effettuando localmente attività di ripristino.
- Un disastro di secondo livello può coinvolgere diversi uffici. Le operazioni di routine possono essere distrutte ed i processi critici dovranno essere eseguiti in altri uffici. Il personale dell'ufficio potrebbe avvalersi dell'assistenza di soggetti esterni.
- Un disastro di terzo livello può coprire una vastissima zona, ad esempio una regione; tipici esempi di questi eventi straordinari sono: inondazioni, terremoti o uragani. In questo caso sono richieste risorse esterne ed assistenza, ma il ripristino completo può richiedere settimane o mesi. Generalmente un disastro di questo livello comporta il blocco dell'operatività dei sistemi.

I sistemi devono essere classificati secondo le definizioni seguenti:

- **Critici**. Le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto.

- **Vitali**. Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici; conseguentemente il costo di un'interruzione è inferiore, anche perché queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

- **Delicati**. Queste funzioni possono essere svolte manualmente, a costi tollerabili, per un lungo periodo di tempo. Benché queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

- **Non-critici.** Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un costo modesto, o nullo, e si richiede un limitato sforzo di riattivazione quando il sistema viene ripristinato.

A fronte delle precedenti considerazioni, in caso di eventuali avvenimenti straordinari, devono essere rispettate le seguenti regole:

- le procedure applicative, il software di sistema e gli archivi che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente;
- il piano d'emergenza deve prevedere il ripristino di tutte le funzioni e non solo i servizi informatici centrali;
- per assicurare la continuità dei servizi devono essere valutate le strategie di ripristino più opportune quali:
  - siti alternativi;
  - metodi di back up;
  - sostituzione dei sistemi hardware di elaborazione;
  - ruoli e responsabilità dei gruppi tecnici di lavoro.

3.9 Conformità

Gli obiettivi di questa linea guida sono:

- garantire il rispetto delle leggi civili, penali, obblighi statutari, regolamentari o contrattuali e di qualsiasi requisito di sicurezza;
- garantire il rispetto di tutte le direttive ministeriali, degli organi di orientamento tecnico e di standardizzazione per l'informatizzazione e la qualità
- assicurare la conformità dei sistemi con i criteri e gli standard di sicurezza nazionali ed internazionali.

4.0 Natura e trattamento dati soggetti afferenti AOU - Cagliari

Il presente DPS disciplina, tra le altre cose, le modalità di trattamento dei dati personali ed "identificativi" relativi al personale medico, sanitario-infermieristico, tecnico, amministrativo, ai collaboratori esterni ed agli studenti della Facoltà di Medicina.
Tali dati sono oggetto di trattamento da parte delle competenti Strutture della AOU – Cagliari e Università degli Studi di Cagliari , ad opera dei soggetti ivi incaricati, con modalità sia manuale, cartacea che informatizzata.

Del personale medico, sanitario-infermieristico, tecnico, amministrativo, collaboratori esterni potranno essere acquisite le seguenti informazioni:

- dati anagrafici, identificativi e informativi contenuti nei curricula e schede personali;
- altri dati diversi da quelli anagrafici contenuti nel fascicolo individuale del personale e dei collaboratori esterni;
- dati contenuti nei certificati medici per giustificazione di assenze (malattie, infortuni ecc.);
- dati inerenti lo stato di salute per esigenze di gestione del personale, assunzioni del personale appartenente alle categorie protette, igiene e sicurezza sul luogo di lavoro, equo indennizzo, causa di servizio ecc.;
- dati relativi alle carriere;
- dati relativi agli stipendi ed alle voci retributive;
- dati relativi alla adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;
- dati relativi ai riscatti ed alle ricongiunzioni previdenziali, dei trattamenti assicurativi e previdenziali obbligatori e contrattuali.

Degli studenti Facoltà di Medicina potranno essere acquisite le seguenti informazioni:

- dati anagrafici, identificativi e informativi contenuti nella domanda di iscrizione;
- dati relativi agli esiti scolastici, intermedi e finali o comunque connessi alla carriera universitaria;
- dati relativi agli studenti diversamente abili o ad elementi reddituali ai fini di eventuali esoneri dal versamento delle tasse universitarie;.

Si precisa che il trattamento di tutti i dati sopra citati avviene esclusivamente ai fini dell'adempimento delle prescrizioni di legge anche relative al rapporto di lavoro e di quelli connessi agli oneri fiscali e previdenziali, secondo quanto disposto sia dalla legislazione vigente in materia, sia dai contratti collettivi nazionali ed integrativi, ovvero per finalità di gestione amministrativa e/o per finalità didattiche e/o per finalità connesse alle eventuali collaborazioni esterne da parte di collaboratori o professionisti presso le strutture dell'Azienda.

Il conferimento dei dati su indicati è dunque obbligatorio.

Si precisa, altresì che i trattamenti sopra menzionati possono riguardare anche i dati:

a) definiti "*giudiziari*" ai sensi dell'art. 4 comma 1 lettera e) del D.lgs 196/2003 e cioè: dati personali idonei a rivelare i provvedimenti di cui all'art. 3 comma 1 lettere da a) a o) e da r) a u) del d.p.r. 14 novembre 2002 n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o indagato ai sensi degli art. 60 e 61 del c.p.p.
b) definiti "*sensibili*" ai sensi dell'art. 4 comma 1 lett. d) del D.lgs 196/2003.

In questa categoria rientrano in particolare:

- i dati relativi all'iscrizione ai sindacati, ai fini dell'effettuazione delle trattenute e del versamento del contributo al sindacato indicato dal dipendente;
- i dati inseriti nelle certificazioni mediche, ai fini della verifica dell'attitudine a determinati lavori, dell'idoneità al servizio, dell'avviamento al lavoro degli inabili;
- i dati relativi allo stato di salute dei dipendenti assunti sulla base della L. 2 aprile 1968 n. 482 e successive modifiche;

- i dati relativi all'appartenenza ad organizzazioni o fedi religiose ai fini dei permessi per festività.
- dati relativi al personale o agli studenti del Polo Universitario diversamente abili ai fini di eventuali esoneri da contributi, tasse od altri oneri previsti per legge o da specifico regolamento.

Tutti i dati relativi al personale medico, sanitario-infermieristico, tecnico, amministrativo o esterno, potranno essere comunicati solo ad enti pubblici o a pubbliche amministrazioni che per legge ne abbiano titolo.

La AOU - Cagliari cura il trattamento dei dati personali del personale dipendente .
Nell'ambito dei suddetti dati personali sono individuati come dati sensibili e/o giudiziari, ai sensi della normativa vigente e coerentemente con quanto sopra indicato, i dati relativi a:

- buste paga (iscrizione al sindacato, indicazione delle categorie protette, assicurazione sanitaria, ecc.
- dati sanitari connessi ad attività di ricerca e clinica
- dati personali del personale (ad. es. dati giudiziari)
- dati relativi ad esoneri contributivi
- dati relativi a soggetti appartenenti a famiglie meno abbienti, eventuali corsi di formazione per categorie disagiate o speciali, ecc.)

5.0 Distribuzione dei compiti e delle responsabilità

5.1 Compiti e responsabilità

Inoltre, sono state individuate le strutture preposte al trattamento dei dati nonché l'elenco dei dati gestiti da ciascuna struttura. Al vertice di ciascuna struttura c'è il responsabile del trattamento dei dati che coincide con il responsabile di servizio. I responsabili del trattamento dei dati personali gestiti dalla struttura assegnata sono nominati con apposito provvedimento del Direttore Generale.
Il Titolare, e le figure individuate come Responsabili, assicureranno che il programma di sicurezza sia adeguatamente sviluppato, realizzato e mantenuto aggiornato e conforme alla legge sulla privacy e alle prescrizioni del presente documento.

Essi, nell'ambito della propria organizzazione, opereranno in modo da:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche, archivi informatici o cartacei contenenti dati personali,
- minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali,
- minimizzare la probabilità che i trattamenti dei dati personali siano modificati senza autorizzazione.

5.2 Il Titolare del trattamento dei dati personali.

L'AOU - Cagliari, nella persona del *Direttore Generale*, è il *Titolare del Trattamento dei dati personali* mediante l'ausilio dei mezzi informatici o cartacei. Nel raccogliere i dati personali (direttamente dall'interessato od anche attraverso la cessione da parte di altri) decide come ed in

base a quali finalità (ad esempio per rapporto di lavoro, per finalità di prevenzione, cura e salute, per finalità didattica, etc.) effettuerà il trattamento dei dati raccolti.

5.3 Il Responsabile del trattamento dei dati personali

L'AOU - Cagliari, nella persona del Direttore Generale, nomina, con propri atti, *Responsabili del trattamento dei dati:*

A) Nell'ambito della Direzione Generale:

- I **Responsabili degli Uffici di Staff**.

Sono Uffici di Staff:

• Affari Generali e Legali	Dr. Ennio Filigheddu
• Programmazione e Controllo	Dr.ssa Simona Cuneo
• Relazioni e comunicazione Aziendale	Sig. Luca Clemente
• Sistemi informativi	Ing. Andrea Casanova
• Programmazione e verifica qualità Risk Management	
• Assistenza infermieristica ostetrica e delle professioni tecnico sanitarie	

B) Nell'ambito delle Direzioni Operative:

- Il **Direttore Amministrativo**, relativamente al complesso dei dati trattati dagli Uffici afferenti alla Direzione Amministrativa;
- Il **Direttore Sanitario**, relativamente al complesso dei trattamenti dei dati socio-sanitari negli ambiti operativi in cui è strutturata l'Azienda**;**
- I responsabili delle strutture così individuate nel seguente elenco

Unità Operative P.O. S.Giovanni di Dio	**Responsabile**
Direzione di Presidio	Dott. Giuseppe Lo Pinzino
Farmacia	Dr.ssa Wanda Lai
Farmacologia clinica	Prof.ssa Maria del Zompo
Dermatologia	Prof. Nicola Aste
Oculistica	Prof. Maurizio Fossarello
Elettrofisiologia della visione	Dott. Rolando Sorcinelli
Patologia chirurgica	Prof. Giampaolo Farina
Clinica chirurgica	Prof. Alessandro Uccheddu
Endoscopia Digestiva	Dott.ssa Pasquala Ledda
Pronto soccorso	Dott.ssa Rosanna Laconi
Istituto di Anatomia patologica	Prof. Gavino Faa
Diabetologia	Dott. Perpaolo Contini
Otorinolaringoiatria	Prof. Ernesto B. Proto
Anestesia e Rianimazione	Dott. Marco Piga
Ostetricia e Ginecologia	Prof. Gian Benedetto Melis
Medicina interna 1	Dott. Mario Brundu
Medicina interna 2	Prof. Luigi Pascalis

Unità Operative P.O. S.Giovanni di Dio	Responsabile
Radiologia	Prof. Giorgio Mallarini
Laboratorio analisi	Dott. Ferdinando Coghe
Cardiologia	Prof. Luigi Meloni
Emodinamica	Dott. Raimondo Pirisi
Istituto di Anestesia e Rianimazione	Prof. Michele Tupputi

Unità Operative Complesso Pediatrico	Responsabile
Pediatria	Prof. Stefano De Virgiliis
Patologia neonatale e Puericultura	Prof. Vassilios Fanos
Neuropsichiatria infantile	Prof. Carlo Cianchetti

Unità Operative P.O. Policlinico Monserrato	Responsabile
Neurofisiopatologia	Prof. Francesco Marrosu
Analisi Chimico Cliniche	Prof.ssa Rosa Cristina Coppola
Microbiologia	Prof. Aldo Manzin
Anatomia Patologica	Prof. Giuseppe Santa Cruz
Medicina Interna-Allergologia ed Immunologia Clinica	Prof. Paolo Emilio Manconi
Cardiologia ed Angiologia	Prof. Giuseppe Mercuro
Chirurgia Generale	Prof. Angelo Nicolosi
Patologia Colon e Retto	Prof. Giuseppe Casula
Anestesia e Rianimazione	Prof. Gabriele Finco
Medicina Interna e Emocoagulopatie	Prof. Francesco Marongiu
Neurologia	Prof.ssa Maria Giovanna Marrosu
Endocrinologia	Prof. Stefano Mariotti
Diabetologia	Prof. Marco Baroni
Medicina preventiva dei lavoratori e Fisiopatologia Respiratoria	Prof. Plinio Carta
Medicina Interna-Malattie del fegato	Prof.ssa Patrizia Farci
Medicina Interna-Malattie metaboliche	Prof. Aldo Solinas
Gastroenterologia	Prof. Luigi Demelia
Endoscopia digestiva	Prof. Paolo Usai
Medicina del Lavoro	Prof. Francesco Sanna Randaccio

Unità Operative P.O. Policlinico Monserrato	Responsabile
Medicina Legale	Prof. Ernesto D'Aloja
Medicina nucleare	Prof. Mario Piga
Oncologia Medica 1	Prof. Giovanni Mantovani
Oncologia medica 2	Prof. Bruno Massidda
Radiodiagnostica	Prof. Giorgio Mallarini
Reumatologia	Prof. Alessandro Mathieu
Patologie Osteomuscolari	Prof. Quirico Mela

Unità Operative Complesso Odontostomatologico	Responsabile
Odontostomatologia	Prof. Vincenzo Piras

C) Nell'ambito delle Aree di Gestione:

Dirigenti e **Responsabili** delle Unità Operative di:

- Provveditorato ed acquisti — Dr.ssa Maria Teresa Piras
- Contabilità e bilancio — Dr. Giuseppe Sau
- Amministrazione del personale — Dr.ssa Maria Luisa Mastino
- Servizio tecnico — Ing. Valter Cossellu
- Tecnology Assessment

5.4 Amministratore di sistema

L'amministratore di sistema è la persona fisica a cui è conferito il compito di sovrintendere alle risorse di un sistema di base dati e di consentirne l'utilizzazione e comunque responsabili di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.
Ai fini della sicurezza e necessario individuare un l'amministratore di sistema all'interno di ogni U.O. clinica. Le responsabilità specifiche saranno indicate nella lettera di incarico.
Relativamente alla gestione dati affidata a società terze il Titolare del trattamento dati si impegna ad ottenere la lista degli "amministratori di sistema" che gestiscono tali trattamenti e l'attestazione scritta che tali soggetti possiedono le caratteristiche richieste dalla vigente normativa in merito.

5.5 L'Incaricato del trattamento dei dati personali

L'Incaricato è colui che operativamente effettua i "trattamenti", attenendosi alle istruzioni del Titolare o del Responsabile.
La AOU - Cagliari affida ai Responsabili il compito di nominare "incaricati " le persone fisiche, in relazione alle attività (e quindi ai trattamenti di competenza), svolte nell'ambito della struttura sanitaria, amministrativa o tecnica di appartenenza, impartendo loro adeguate istruzioni.

6.0 Organigramma

Il documento denominato "Atto Aziendale – Organigramma e l'Azienda AOU - Cagliari" illustra nel particolare le Unità Operative (U.O.) unitamente alle funzioni, alle responsabilità ed agli ambiti di trattamento dei dati personali.
Tramite apposito modulo prestampato, diffuso dal Titolare del trattamento dati e compilato dal Responsabile delle U.O., è in corso la raccolta dei nominativi dei dipendenti da individuare come "Incaricato del trattamento dei dati personali".
Si allega al presente DPS copia di tale modulo.

7.0 Risorse del Sistema Informativo Sanitario per il trattamento dati

I dati sono archiviati presso la sede del CRESSAN il titolare dei dati con specifico atto di nomina, in esecuzione di quanto stabilito con decreto del Presidente della Giunta Regionale n. 1394/1 del 9 luglio 2003; ha nominato il Raggruppamento Temporaneo di Imprese (in breve anche RTI), composto da Engineering Sanità Enti Locali S.P.A. e Telecom Italia S.p.a., **Responsabile del Trattamento dei dati**, effettuato con strumenti elettronici o comunque automatizzati, nella persona del legale rappresentante in possesso dei requisiti "indispensabili" individuati dall'art. 29 D.Lgs, 196/2003.
RTI attraverso la firma per accettazione dell'atto di nomina sopra citato redatto secondo quanto disposto dall'art. 29 del codice (si allega al presente documento per farne parte integrante), si impegna al trattamento dei dati secondo quanto stabilito dalla normativa vigente

Il Sistem Informativo Sanitario denominato SISAR dell'AOU - Cagliari è dettagliatamente descritto nel documento progettuale del relativo appalto pubblico.

In tale documento, descrive l'architettura dei sistemi di elaborazione e di trasmissione delle informazioni trattate dall'AOU – Cagliari in particolare, si riportano informazioni relative a:

1) rete di trasmissisone dati;
2) sistema di elaborazione server;
3) sistema di elaborazione client;
4) software applicativi-gestionali;
5) data-base;
6) sistema della sicurezza informatica;

Pertanto, si rimanda al documento progettule sopra riportato nonché alle documentazioni di progettazione esecutiva con particolare attenzione all'architettura dei sistemi preposti al trattemnto dei dati personali con criteri e meccanismi di garanzia della sicurezza, secondo le attuali disponibilità tecnologiche.

Ad integrazione si allega lo schema ***(Schema 1)*** della rete aziendale in essere alla data di compilazione del presente documento.

7.1 Analisi e classificazione minacce e vulnerabilità

Una minaccia è la causa potenziale di un evento non desiderato che può avere come conseguenza danni per l'AOU – Cagliari e per i suoi asset, ovvero beni informativi e per le attività che prevedono un trattamento di dati.

Gli eventi inerenti alla minaccia possono essere naturali, intenzionali e accidentali ed il suo verificarsi, cioè l'attuarsi di una minaccia, può consistere in:

- distruzione di un asset
- corruzione o modifica di un asset
- sottrazione o perdita di un asset
- pubblicazione di informazioni riservate
- uso non lecito di un asset
- interruzione del servizio

Il verificarsi dell'evento e, quindi, l'attuarsi della minaccia, possono essere agevolati da un insieme di vulnerabilità, ovvero da un insieme di condizioni, punti deboli degli asset, che possono consentire ad una minaccia di influire su un asset.

Tipicamente una vulnerabilità è conseguenza di:

- un'errata procedura (informatica e/o organizzativa),
- personale non sufficientemente addestrato,
- tecnologie non correttamente configurate o tecnologie difettose.

La rilevazione delle vulnerabilità rispetto alle minacce consente:

- la misurazione del livello di pericolosità di una minaccia rispetto ai sistemi e beni informativi;
- la classificazione esaustiva delle minacce da considerare nel piano della sicurezza
- l'analisi e la rilevazione nella successiva fase di redazione del DPS di nuove vulnerabilità e, conseguentemente delle potenziali minacce ad esse associate non considerate nella versione precedente del documento.

8.0 Regolamento per l'utilizzo della rete

8.1 Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

8.2 Principi generali - diritti e responsabilità

AOU - Cagliari promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità. Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.
Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri

operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

8.3 Abusi e attività vietate

E' vietato ogni tipo di abuso. In particolare è vietato:

- usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- utilizzare la rete per scopi incompatibili con l'attività istituzionale;
- utilizzare una password a cui non si è autorizzati;
- cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;
- conseguire l'accesso non autorizzato a risorse di rete interne o esterne;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri, trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- rimuovere, danneggiare deliberatamente o asportare componenti hardware.
- utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;
- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

8.4 Attività consentite

E' consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

8.5 Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.
L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.
Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili, l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.
L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

8.6 Modalità di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.
L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.
L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.
L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.
Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password.

9.0 Video sorveglianza

Nell'esercitare attività di videosorveglianza, viene rispettato il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati, solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- è scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
- il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai i 5 giorni;

la conservazione dei dati oltre il termine previsto alla lettera d), è possibile solo in relazioni al verificarsi di illeciti o quando siano in corso indagini giudiziarie;
i dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.

Il Regolamento viene integrato dalla seguente immagine:

10.0 Monitoraggio del piano

10.1 Monitoraggio e validazione del piano di sicurezza

La fase di monitoraggio e validazione della metodologia prevede che venga verificata dal responsabile del trattamento dei dati, o dai suoi delegati, o da un gruppo appositamente costituito, la corretta attuazione del piano di lavoro.
Le schede di attuazione e monitoraggio del DPS consentono sia di controllare lo stato di attuazione delle misure di sicurezza, sia di monitorare tutti gli eventi di interesse per la sicurezza. Il responsabile del trattamento dei dati (o i suoi delegati), redigerà tali schede, con **frequenza semestrale o annuale** dall'approvazione del DPS da parte del Titolare del trattamento dei dati.

10.2 Schede di attuazione

E' stata predisposto la seguente scheda:

Elemento di controllo	Cosa controllare	Esito
Responsabile del trattamento	Esiste l'atto di nomina? (s/n)	
Responsabile del trattamento	Esistono altri candidati al ruolo? (s/n)	
Responsabile del trattamento	Se esistono altri candidati al ruolo, chi sono?	
Incaricati al trattamento	Esistono atti di incarico nominali? (s/n)	
Incaricati al trattamento	Esiste un elencazione degli incaricati dalla quale è possibile rilevare nominativi ed ambiti di trattamento, in modo da rilevare compiti e responsabilità? (s/n)	
Incaricati al trattamento dati	Sono stati individuati gli ambiti di trattamento? (s/n)	
Incaricati al trattamento dati	Gli ambiti di trattamento corrispondono alle reali esigenze aziendali ed alle posizioni organizzative, come da organigramma? (s/n)	
Incaricati al trattamento dati	Sono state rilevate esigenze di variazione di ambiti di trattamento? (s/n)	
Incaricati al trattamento dati	Sono state rilevate esigenze di aggiornare l'elenco degli incaricati? (s/n)	
Incaricati al trattamento dati	E' stato individuato l'addetto alla gestione delle risorse elettoniche? (s/n)	
Incaricati al trattamento dati	E' stato fornito a tutti un elenco di istruzioni operative per gli scopi di sicurezza nel trattamento dei dati? (s/n)	
Incaricati al trattamento dati	E' stata pianificata la formazione? (s/n)	
Incaricati al trattamento dati	E' stata erogata la formazione a tutti gli incaricati? (s/n/parzialmente)	
Incaricati al trattamento dati	E' stata prevista della formazione per i nuovi ingressi o per cambiamento di mansione? (s/n/parzialmente)	
Responsabili/Incaricati al trattamento dati	Esistono incarichi per soggetti esterni? (s/n)	
Responsabili/Incaricati al	L'elenco degli incarichi, corrisponde all'elenco	

Elemento di controllo	Cosa controllare	Esito
trattamento dati	dei soggetti esterni per il trarramento dei dati? (s/n; indicare le anomalie)	
Analisi dei rischi	E' stata effettuata l'analisi dei rischi, rispetto alle vulnerabilità ed alle minacce descritte nel DPS? (s/n/parzialmente)	
Analisi dei rischi	Sono stati rilevati nuovi eventi minacciosi, individuandone le vulnerabilità, nelle schede di registrazioen eventi? (s/n/parzialmente)	
Analisi dei rischi	Sono stati decritti gli eventi minacciosi nuovi, in modo da riportarli nella scheda minacce e vulnerabilità (indoicare sinteticamente gli eventi o i riferimenti delle schede di tracciatura)	
Analisi dei rischi	A minace individuate corrispondono anche i relativi trattamenti (misure di sicurezza)? (s/n)	
Analisi dei rischi	I trattamenti individuati sono attualizzati (s/n)	
Trattamenti dati	Esiste una procedura o un meccanismo riconosciuto per i criteri e le modalità di ripristino dei dati (s/n; indicare evntauli note)	
Procedura di controllo degli accessi	Si attua (s/n/problematiche)	
Procedura di gestione degli account	Si attua (s/n/problematiche)	
Procedura di gestione del materiale in entrata ed in uscita	Si attua (s/n/problematiche)	
Procedura di manutenzione degli apparati	Si attua (s/n/problematiche)	
Procedura di gestione della rete	Si attua (s/n/problematiche)	
Procedure di attuazione delle norme vigenti inerenti alla sicurezza dell'edificio e del personale	Si attua (s/n/problematiche)	
Procedure operative per la gestione di eventi straordinari	Si attua (s/n/problematiche)	
Scheda Anomalie riscontrate	Sono utilizzare per la registrazione (s/n)	

Per gli eventi non previsti nel piano di sicurezza, il responsabile del trattamento dei dati, o suoi delegati, individuerà comunque quali attività porre in essere per risolvere l'evento di rischio.

11.0 Pianificazione degli interventi formativi

Sono stati previsti interventi formativi per i dipendenti per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

attraverso la formazione ci si propone di far acquisire al personale le competenze necessarie per la messa in atto di procedure, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
Gli interventi sopra menzionati, si configurano come aggiornamento obbligatorio per i dipendenti dell'Azienda, saranno gestiti dall'Ufficio Formazione che ne curerà i contenuti, la calendarizzazione, la banca dati dei partecipanti e la certificazione

In questa sezione si riportano le informazioni necessarie per individuare il quadro degli interventi formativi che si prevede di svolgere:

- Corso base privacy per tutto il personale attualmente in carico
- Corso base privacy per i nuovi assunti
- Corso avanzato privacy per amministratori di sistema e incaricati trattamento dati

.

La formazione si intende preventiva al trattamento dei dati.

Si precisa che il presente DPS costituisce parte integrante della formazione del personale attivo in questa Azienda Sanitaria.

12.0 Evoluzione del DPS

A partire dalla scheda di monitoraggio periodicamente saranno rivisti i requisiti di sicurezza e quindi si provvederà all'introduzione di nuovi ed opportuni elementi correttivi per la redazione di un nuovo Piano di sicurezza nel DPS.
La redazione del nuovo DPS sarà, in ogni caso, effettuata con una frequenza annuale, entro la scadenza prevista per legge, fissata al 31 Marzo di ogni anno.
In questa fase sarà formulato un rapporto contenente una classificazione delle variazioni del nuovo piano di sicurezza rispetto al precedente, secondo i seguenti parametri:

- Variazioni della struttura organizzativa, logistica e tecnica
- Analisi e classificazione dei processi interessati
- Classificazione minacce, vulnerabilità e valutazione del rischio
- Variazioni delle procedure operative.

Allegato 1 : Lettera di incarico **Responsabile trattamento Dati**

Oggetto: Incarico di responsabile del trattamento dati.

Il sottoscritto ***[Titolare]***, titolare del trattamento dei dati dell'Azienda Ospedaliero Universitaria di Cagliari, ai sensi del D.L.vo N. 196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", affida al Sig. ***[Incaricato]*** l'incarico di responsabile del trattamento dei dati con i seguenti compiti:

- ***Compiti ed istruzioni per il Responsabile del Trattamento dei Dati Personali***

in applicazione
del "Codice in materia di protezione dei dati personali" (D.Lgs.n. 196/2003)

1. PRINCIPI GENERALI DA OSSERVARE

Ogni *trattamento* di dati personali deve avvenire, nel rispetto dei seguenti **principi di ordine generale**:

Ai sensi dell'art. 11 del Codice, che prescrive le "*Modalità del trattamento e requisiti dei dati",* per ciascun trattamento di propria competenza, il Responsabile del Trattamento deve fare in modo che i dati siano trattati:

- secondo il principio di **liceità,** ossia conformemente alle disposizioni del Codice, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal **principio fondamentale di riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Codice è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

Ciascun **Responsabile** deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste **sanzioni penali** (artt. 167 e ss.).
In ogni caso la **responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Mentre, in merito alla **responsabilità civile,** si fa rinvio all'art. 15 del Codice, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

2. COMPITI PARTICOLARI DEL RESPONSABILE

Il **Responsabile** del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare**:

A) identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività di test del Sistema ADT (Accettazione, Dimissione, Trasferimento) come descritte nel progetto per la realizzazione del SISaR e costituenti l'oggetto del contratto d'appalto aggiudicato al RTI con Determinazione n° 603 del 26/09/2007.

B) attenersi rigorosamente, per ciascun trattamento di dati personali e/o sensibili, relativo all'attività di test del Sistema ADT, a quanto previsto nel progetto per la realizzazione del SISaR.

C) definire, per ciascun trattamento di dati personali e/o sensibili, la **durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

D) assicurarsi che il trattamento dei dati sensibili e giudiziari (art. 20 - 21 e 22 del Codice) che riguardano prestazioni di carattere sanitario avvenga solo limitatamente ai tipi di dati e di operazioni identificati con il Decreto del Presidente della Regione Sardegna, 3 ottobre 2007, n. 5, recante il "Regolamento per il trattamento dei dati sensibili e giudiziari".

E) assicurare che la **comunicazione a terzi** e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali.

F) adempiere agli **obblighi di sicurezza**, quali:

- adottare le **misure minime di sicurezza** espressamente previste dal Codice della Privacy. Tra queste ultime, in particolare, si segnala l'obbligo (lett. g – art. 34) di collaborare con il Titolare alla stesura e aggiornamento annuale del

Documento Programmatico sulla Sicurezza (DPS), nelle modalità di volta in volta indicate.

- adottare tutte le **preventive misure di sicurezza**, ritenute **idonee** al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31);
- **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito, o non conforme alle finalità istituzionali.

G) far osservare gli adempimenti previsti in caso di **nuovi trattamenti** e **cancellazione** di trattamenti*:*

- in particolare, comunicare preventivamente al Titolare l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice;
- segnalare al Titolare l'eventuale cessazione di trattamento.

H) proporre al Titolare del trattamento dei dati la nomina di soggetti esterni quali Responsabili del trattamento dati in relazione all'affidamento agli stessi di determinate attività, nell'ambito dei compiti istituzionali dell'Amministrazione.

I) collaborare con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal D. Lgs. 196/2003 e segnalare eventuali problemi applicativi.

J) trasmettere le richieste degli interessati al titolare, al fine di garantire l'esercizio dei diritti dell'interessato, ai sensi degli artt. 7, 8, 9 e 10 del D. Lgs. 196/2003.

K) collaborare con il Titolare per l'evasione delle richieste degli interessati ai sensi dell'art. 10 del D. Lgs. 196/2003 e delle istanze del Garante per la protezione dei dati personali.

3. MISURE DA ADOTTARE NEI CONFRONTI DEGLI INCARICATI.

A) **Individuare**, tra i propri collaboratori, designandoli per iscritto, **gli Incaricati** del trattamento;

B) **recepire le istruzioni** cui devono attenersi gli Incaricati nel trattamento dei dati impartite dal Titolare, assicurandosi che vengano materialmente consegnate agli stessi o siano già in loro possesso, unitamente al "**Regolamento per l'utilizzo dei servizi informatici aziendali**";

C) **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli incaricati del trattamento, curando in particolare il profilo della **riservatezza**, della **sicurezza di accesso** e della **integrità dei dati** e l'osservanza da parte degli Incaricati, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;

D) stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli Incaricati, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini del **riscontro** di eventuali richieste di esecuzione dei diritti di cui all'art. 7.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Una copia del presente atto di nomina dovrà essere restituita al Titolare, debitamente firmato per accettazione dall'RTI, nella persona del suo legale rappresentante.

Il Direttore Generale Azienda AOU - Cagliari

_____

Il Legale Rappresentante RTI

_____

Data

Allegato 2 : Lettera di incarico ***Amministratore di sistema***

Oggetto: Incarico di amministratore di sistema.

Il sottoscritto ***[Titolare]***, titolare del trattamento dei dati dell'Azienda Ospedaliero Universitaria di Cagliari, ai sensi del D.L.vo N. 196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", e al provvedimento del garante del 27.11.2008 "*Misure ed accorgimenti prescritti ai titolari dei trattamenti effetuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" modificato in data 25.06.2009, affida al Sig. ***[Incaricato]*** l'incarico di amministratore di sistema con i seguenti compiti:

- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- fare in modo che sia prevista la disattivazione dei codici indentificativi personali, in caso di perdita della qualità che consentiva all'incaricato l'accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;
- gestire le password della propria unità operativa
- collaborare con il responsabile del trattamento dei dati personali
- informare il responsabile della sicurezza informatica sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.
- *[Altri eventuali compiti specifici]*

L'amministratore testé incaricato dichiara di essere a conoscenza di quanto stabilito dal D.L.vo N. 196 del 30/06/2003 ed in particolare di quanto indicato nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme descritte nel Documento Programmatico sulla Sicurezza, in relazione ai compiti sopra indicati.

Per conoscenza ed accettazione
[Incaricato]

_____
(firma)

Il titolare del trattamento
[Titolare]

_____
(firma)

Allegato 3 : Lettera incarico ***Incaricati trattamento dati***

Oggetto: Lettera di incarico al trattamento dei dati.

Il sottoscritto ***[Titolare]***, responsabile del trattamento dei dati, della struttura ***[Struttura]***, dell'Azienda Ospedaliero Universitaria di Cagliari ai sensi del D.L.vo N. 196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", conferisce al Sig. [**Incaricato**] nato a [Nascita] il [DataNascita] l'incarico di compiere le operazioni di trattamento dei dati sotto elencate, nell'ambito delle funzioni di **(indicare le mansioni)** che é chiamato a svolgere, con l'avvertimento che dovrà operare osservando le direttive del titolare /responsabile.

A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal Titolare/Responsabile riportate nel documento programmatico sulla sicurezza;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
  - divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del titolare/responsabile;
  - l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
  - la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del responsabile del trattamento dei dati;non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti

contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;

qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Operazioni di trattamento dei dati cui può accedere [Incaricato]

(elenco delle operazioni)

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.
Per ogni altra misura ed istruzione qui non prevista ci si richiama al Documento Programmatico sulla Sicurezza.

Per conoscenza ed accettazione
[Incaricato]

_____
(firma)

Il titolare del trattamento
[Titolare]

_____

Allegato 4 : Lettera incarico *responsabile esterno trattamento dati*

Oggetto: Nomina a responsabile esterno per il trattamento dei dati personali nell'ambito del progetto per l'informatizzazione del sistema sanitario regionale (progetto SISaR).

IL DIRETTORE GENERALE

nella persona del legale rappresentante _____ della Azienda Ospedaliero Universitaria di Cagliari in qualità di Titolare del trattamento dei dati (D.lgs. 196/03):

- visto il Decreto Legislativo 30 giugno 2003, n. 196. "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- preso atto che l'art. 4, comma 1, lettera g) del suddetto Decreto definisce il "Responsabile" come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali;
- atteso che l'art. 29, commi 2, 3, 4 e 5 del D. Lgs. n. 196/2003 dispone che: "*2. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. 3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione dei compiti. 4. I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare. 5. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni*";
- vista la Legge Regionale N. 10 del 28/07/2006: Tutela della salute e riordino del servizio sanitario della Sardegna – Abrogazione della Legge Regionale del 26/01/1995 N. 5;
- visto il Piano Regionale dei Servizi Sanitari della Regione Sardegna 2006 - 2008, approvato dalla Giunta Regionale con delibera 51/9 del 4 novembre 2005;

- visto il Piano Nazionale di contenimento dei tempi di attesa per il triennio 2006-2008, approvato in Conferenza Stato-Regioni - 03/04/2006 e relative implicazioni sulle soluzioni applicative CUP per la specialistica ambulatoriale e per i ricoveri ospedalieri;

- visto il Piano sanitario nazionale 2006-2008 e Accordo Stato Regioni del 24 luglio 2003 e del 29 luglio 2004 relativamente alle priorità Sviluppo della politica dei LEA e cure primarie11;

- visto il Piano Regionale di contenimento dei tempi e liste di attesa per il triennio 2006-2008, di cui all'art. 1, comma 280 della Legge 23.12.2005 n. 266 – Delibera Giunta Regionale 28/15 del 27/6/2006;

- vista la Normativa nazionale e regionale relativa ai flussi obbligatori del SSN;

- vista la Delibera della Giunta Regionale N. 32/4 del 13/07/2005 “Piano per l’informatizzazione del Sistema Sanitario Regionale”;

- vista la Delibera della Giunta Regionale N. 34/28 del 2 agosto 2006 “Progetto per l’informatizzazione del sistema sanitario regionale”;

- visto il D. Lgs n. 42 del 28 febbraio 2005 "Istituzione del Sistema pubblico di connettività e della Rete internazionale della pubblica amministrazione, a norma dell'art. 10, della L. 229 del 29 luglio 2003" (G.U. del 30 marzo 2005, nr. 73);

- visto il D. lgs n. 82 del 7 marzo 2005 “Codice dell’amministrazione digitale”;

- considerate la “Strategia architetturale per la Sanità Elettronica” e la “Politica per la Sanità Elettronica”, prodotte dal Tavolo permanente per la Sanità Elettronica;

- considerata la convenzione nazionale Medici di Medicina Generale e quella per la Pediatria di Libera Scelta e i relativi recepimenti in ambito regionale e aziendale;

- vista la Delibera del 02/08/2006, n. 34/28, relativa al Progetto per l’informatizzazione del sistema sanitario regionale (progetto SISaR);

- vista la Delibera del 08/08/2006, n. 35/18, relativa al Progetto per l’informatizzazione del sistema sanitario regionale. Rettifica deliberazione n. 34/28 del 02/08/2006;

- visto il Bando per l’appalto per la realizzazione del SISaR: determina n° 836 del 10/08/2006 del dirigente del Servizio affari generali e istituzionali e sistema informativo della Direzione generale della sanità (Pubblicazione Bando sulla GUCE 2006 /S 156 - 168659 del 18/08/2006);

- considerato che il Servizio affari generali e istituzionali e sistema informativo della Direzione generale della sanità della Regione Autonoma della Sardegna ha provveduto, con Determinazione n° 836 del 10/08/2006, all’espletamento dell’appalto per la realizzazione del Sistema Informativo Sanitario Integrato

Regionale (SISaR) - Pubblicazione Bando sulla GUCE 2006 /S 156 - 168659 del 18/08/2006;

- considerato che il Servizio affari generali e istituzionali e sistema informativo della Direzione generale della sanità della Regione Autonoma della Sardegna ha provveduto, con Determinazione n° 603 del 26/09/2007, all'aggiudicazione dell'appalto medesimo al Raggruppamento Temporaneo di Imprese composto da Engineering Sanità Enti Locali S.P.A., corrente sede in Roma, via San Martino della Battaglia n. 8, P.IVA 09483280153 e Telecom Italia S.p.a. corrente sede in Milano, Piazza degli Affari n. 2, P.IVA 00488410010

- visto il contenuto del progetto per la realizzazione del Sistema Informativo Sanitario Integrato Regionale (SISaR), il quale è in coerenza con quanto previsto dal Piano Sanitario Nazionale 2006 – 2008, dalla proposta di Piano Sanitario Regionale 2006 – 2008, dalla Politica per la Sanità Elettronica e dal Sistema Pubblico di Connettività (SPC);

- considerato che l'obiettivo del progetto SISaR è la realizzazione di un Sistema Informativo Sanitario Integrato Regionale che superi la mancanza di correlazione tra processi e sistemi informatici di governo (informazionali), e tra processi e sistemi di servizio/erogazione (operazionali) in un contesto di necessaria accelerazione dell'informatizzazione estesa dei processi sanitari;

- Considerato che l'infrastruttura ICT delle Aziende USL è complessivamente costituita da differenti tipologie di sistemi e di reti ed è caratterizzata da una connettività limitata tra i vari nodi della rete (in termini principalmente di larghezza di banda e capillarità); che il sistema di connettività infra-aziendale e verso il resto degli attori del territorio regionale è attualmente fortemente disomogeneo e che gli applicativi software utilizzati sono altamente frammentati e di conseguenza scarsamente interoperabili;

- Considerato che il nuovo sistema informativo sanitario regionale dovrà essere progettato e realizzato per erogare in outsourcing a tutte le Aziende sanitarie della Regione da parte del Centro Regionale per i Servizi Sanitari (CRESSAN) i seguenti servizi:

    a) il sistema informativo sanitario direzionale (ivi compreso il sistema informativo epidemiologico);
    b) il sistema informativo gestore risorse – CUP;
    c) il sistema informativo sanitario amministrativo;

- considerato che il nuovo sistema informativo sanitario regionale dovrà essere progettato e realizzato in modo da integrarsi con tutti i sistemi i cui progetti sono in corso di attuazione quali: MEDIR, ANAGS, RTP, Tessera sanitaria, Sistema Informativo Assistenza Sociale, Gestione dei Sert, Gestione degli Screening oncologici, e, ove possibile, con i sistemi clinico – sanitari attualmente presenti nelle Aziende sanitarie.

- considerato che il nuovo sistema informativo sanitario regionale si appoggerà sulla rete telematica regionale e sui servizi di rete ed applicativi messi a disposizione dal Centro Regionale per i Servizi Sanitari (CRESSAN) (connettività, interoperabilità e cooperazione applicativa, sicurezza, autenticazione, autorizzazione, accounting,..).

- Ritenuto che il Raggruppamento Temporaneo di Imprese composto da Engineering sanità, Enti Locali S.p.a. e Telecom Italia S.p.a., in qualità di aggiudicatario dell'appalto pubblico di servizi denominato SISaR, per l'ambito di attribuzioni, funzioni e competenze conferite, abbia i requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza;

- Considerato che, dalla lettura combinata dell'art. 37 del D.lgs. n. 196/03 e del comunicato stampa, esplicativo, pubblicato dall'Autorità Garante il 26 aprile 2004, i titolari coinvolti in attività di trattamento dati "relativi ad una banca dati" o "prestati per via telematica" ovvero "relativi alla fornitura di beni", devono procedere alla notificazione prima dell'inizio del trattamento.

NOMINA

Il Raggruppamento Temporaneo di Imprese (in breve anche RTI), composto da Engineering Sanità Enti Locali S.P.A. e Telecom Italia S.p.a., **Responsabile del Trattamento dei dati**, effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'esclusivo ambito di attività, attribuitegli con il provvedimento di aggiudicazione (Determinazione n° 603 del 26/09/2007) dell'appalto pubblico di servizi denominato SISaR.
Per effetto della presente nomina, il Raggruppamento Temporaneo di Imprese, in qualità di Responsabile del trattamento dei dati, ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le seguenti istruzioni impartite dal Titolare.

Compiti ed istruzioni per il Responsabile del Trattamento dei Dati Personali

in applicazione
del "Codice in materia di protezione dei dati personali" (D.Lgs.n. 196/2003)

4. PRINCIPI GENERALI DA OSSERVARE

Ogni *trattamento* di dati personali deve avvenire, nel rispetto dei seguenti **principi di ordine generale**:

Ai sensi dell'art. 11 del Codice, che prescrive le "*Modalità del trattamento e requisiti dei dati",* per ciascun trattamento di propria competenza, il Responsabile del Trattamento deve fare in modo che i dati siano trattati:

- secondo il principio di **liceità,** ossia conformemente alle disposizioni del Codice, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal **principio fondamentale di riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Codice è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

Ciascun **Responsabile** deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste **sanzioni penali** (artt. 167 e ss.).
In ogni caso la **responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Mentre, in merito alla **responsabilità civile,** si fa rinvio all'art. 15 del Codice, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

5. COMPITI PARTICOLARI DEL RESPONSABILE

Il **Responsabile** del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare**:

L) identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività di test del Sistema ADT (Accettazione, Dimissione, Trasferimento) come descritte nel progetto per la realizzazione del SISaR e costituenti l'oggetto del contratto d'appalto aggiudicato al RTI con Determinazione n° 603 del 26/09/2007.

M) attenersi rigorosamente, per ciascun trattamento di dati personali e/o sensibili, relativo all'attività di test del Sistema ADT, a quanto previsto nel progetto per la realizzazione del SISaR.

N) definire, per ciascun trattamento di dati personali e/o sensibili, la **durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

O) assicurarsi che il trattamento dei dati sensibili e giudiziari (art. 20 - 21 e 22 del Codice) che riguardano prestazioni di carattere sanitario avvenga solo limitatamente ai tipi di dati e di operazioni identificati con il Decreto del Presidente della Regione Sardegna, 3 ottobre 2007, n. 5, recante il "Regolamento per il trattamento dei dati sensibili e giudiziari".

P) assicurare che la **comunicazione a terzi** e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali.

Q) adempiere agli **obblighi di sicurezza**, quali:

- adottare le **misure minime di sicurezza** espressamente previste dal Codice della Privacy. Tra queste ultime, in particolare, si segnala l'obbligo (lett. g – art. 34) di collaborare con il Titolare alla stesura e aggiornamento annuale del Documento Programmatico sulla Sicurezza (DPS), nelle modalità di volta in volta indicate.
- adottare tutte le **preventive misure di sicurezza**, ritenute **idonee** al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31);
- **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito, o non conforme alle finalità istituzionali.

R) far osservare gli adempimenti previsti in caso di **nuovi trattamenti** e **cancellazione** di trattamenti*:*

- in particolare, comunicare preventivamente al Titolare l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice;
- segnalare al Titolare l'eventuale cessazione di trattamento.

S) proporre al Titolare del trattamento dei dati la nomina di soggetti esterni quali Responsabili del trattamento dati in relazione all'affidamento agli stessi di determinate attività, nell'ambito dei compiti istituzionali dell'Amministrazione.

T) collaborare con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal D. Lgs. 196/2003 e segnalare eventuali problemi applicativi.

U) trasmettere le richieste degli interessati al titolare, al fine di garantire l'esercizio dei diritti dell'interessato, ai sensi degli artt. 7, 8, 9 e 10 del D. Lgs. 196/2003.

V) collaborare con il Titolare per l'evasione delle richieste degli interessati ai sensi dell'art. 10 del D. Lgs. 196/2003 e delle istanze del Garante per la protezione dei dati personali.

6. MISURE DA ADOTTARE NEI CONFRONTI DEGLI INCARICATI.

E) **Individuare**, tra i propri collaboratori, designandoli per iscritto, **gli Incaricati** del trattamento;

F) **recepire le istruzioni** cui devono attenersi gli Incaricati nel trattamento dei dati impartite dal Titolare, assicurandosi che vengano materialmente consegnate agli stessi o siano già in loro possesso, unitamente al "**Regolamento per l'utilizzo dei servizi informatici aziendali**";

G) **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli incaricati del trattamento, curando in particolare il profilo della **riservatezza**, della **sicurezza di accesso** e della **integrità dei dati** e l'osservanza da parte degli Incaricati, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;

H) stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli Incaricati, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini del **riscontro** di eventuali richieste di esecuzione dei diritti di cui all'art. 7.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Una copia del presente atto di nomina dovrà essere restituita al Titolare, debitamente firmato per accettazione dall'RTI, nella persona del suo legale rappresentante.

Il Direttore Generale Azienda AOU - Cagliari

_____

Il Legale Rappresentante RTI

_____

Data

Allegato 5

Oggetto: Nomina a responsabile esterno per il trattamento dei dati previdenziali di dipendenti

IL DIRETTORE GENERALE

nella persona del legale rappresentante _____ della Azienda Ospedaliero Universitaria di Cagliari, in qualità di Titolare del trattamento dei dati (D.lgs. 196/03):

- visto il Decreto Legislativo 30 giugno 2003, n. 196. "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- preso atto che l'art. 4, comma 1, lettera g) del suddetto Decreto definisce il "Responsabile" come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali;
- atteso che l'art. 29, commi 2, 3, 4 e 5 del D. Lgs. n. 196/2003 dispone che: "*2. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. 3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione dei compiti. 4. I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare. 5. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni*";
- vista la Delibera della Giunta Regionale N. 32/4 del 13/07/2005 "Piano per l'informatizzazione del Sistema Sanitario Regionale";
- vista la Delibera della Giunta Regionale N. 34/28 del 2 agosto 2006 "Progetto per l'informatizzazione del sistema sanitario regionale";

- visto il D. Lgs n. 42 del 28 febbraio 2005 "Istituzione del Sistema pubblico di connettività e della Rete internazionale della pubblica amministrazione, a norma dell'art. 10, della L. 229 del 29 luglio 2003" (G.U. del 30 marzo 2005, nr. 73);

- visto il D. lgs n. 82 del 7 marzo 2005 “Codice dell’amministrazione digitale”;

- Considerato che, dalla lettura combinata dell’art. 37 del D.lgs. n. 196/03 e del comunicato stampa, esplicativo, pubblicato dall'Autorità Garante il 26 aprile 2004, i titolari coinvolti in attività di trattamento dati “relativi ad una banca dati” o “prestati per via telematica” ovvero “relativi alla fornitura di beni”, devono procedere alla notificazione prima dell’inizio del trattamento.

- Considerato che, L’Azienda Sanitaria Locale n° 8 di Cagliari è materialmente depositaria dei dati previdenziali di Dipendenti dell’AOU – Cagliari

NOMINA

L’Azienda Sanitaria Locale n°8 – Cagliari Responsabile del trattamento dei dati, effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi per l’esclusivo ambito di attività, attribuitegli, che ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le seguenti istruzioni impartite dal Titolare.

Compiti ed istruzioni per il Responsabile del Trattamento dei Dati Personali

in applicazione
del “Codice in materia di protezione dei dati personali” (D.Lgs.n. 196/2003)

7. PRINCIPI GENERALI DA OSSERVARE

Ogni *trattamento* di dati personali deve avvenire, nel rispetto dei seguenti **principi di ordine generale**:

Ai sensi dell’art. 11 del Codice, che prescrive le “*Modalità del trattamento e requisiti dei dati”,* per ciascun trattamento di propria competenza, il Responsabile del Trattamento deve fare in modo che i dati siano trattati:

- secondo il principio di **liceità,** ossia conformemente alle disposizioni del Codice, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all’ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal **principio fondamentale di riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Codice è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

Ciascun **Responsabile** deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste **sanzioni penali** (artt. 167 e ss.).
In ogni caso la **responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Mentre, in merito alla **responsabilità civile,** si fa rinvio all'art. 15 del Codice, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

8. COMPITI PARTICOLARI DEL RESPONSABILE

Il **Responsabile** del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare**:

A) identificare e censire i **trattamenti** di dati personali, le **banche dati** e gli **archivi** gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività

B) attenersi rigorosamente, per ciascun trattamento di dati personali e/o sensibili, al rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

C) definire, per ciascun trattamento di dati personali e/o sensibili, la **durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

D) assicurarsi che il trattamento dei dati sensibili e giudiziari (art. 20 - 21 e 22 del Codice) che riguardano prestazioni di carattere sanitario avvenga solo limitatamente ai tipi di dati e di operazioni identificati con il Decreto del Presidente della Regione Sardegna, 3 ottobre 2007, n. 5, recante il "Regolamento per il trattamento dei dati sensibili e giudiziari".

E) assicurare che la **comunicazione a terzi** e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di

legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali.

F) adempiere agli **obblighi di sicurezza**, quali:

- adottare le **misure minime di sicurezza** espressamente previste dal Codice della Privacy. Tra queste ultime, in particolare, si segnala l'obbligo (lett. g – art. 34) di collaborare con il Titolare alla stesura e aggiornamento annuale del Documento Programmatico sulla Sicurezza (DPS), nelle modalità di volta in volta indicate.

- adottare tutte le **preventive misure di sicurezza**, ritenute **idonee** al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31);
- **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito, o non conforme alle finalità istituzionali.

G) far osservare gli adempimenti previsti in caso di **nuovi trattamenti** e **cancellazione** di trattamenti*:*

- in particolare, comunicare preventivamente al Titolare l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice;
- segnalare al Titolare l'eventuale cessazione di trattamento.

H) proporre al Titolare del trattamento dei dati la nomina di soggetti esterni quali Responsabili del trattamento dati in relazione all'affidamento agli stessi di determinate attività, nell'ambito dei compiti istituzionali dell'Amministrazione.

I) collaborare con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal D. Lgs. 196/2003 e segnalare eventuali problemi applicativi.

J) trasmettere le richieste degli interessati al titolare, al fine di garantire l'esercizio dei diritti dell'interessato, ai sensi degli artt. 7, 8, 9 e 10 del D. Lgs. 196/2003.

K) collaborare con il Titolare per l'evasione delle richieste degli interessati ai sensi dell'art. 10 del D. Lgs. 196/2003 e delle istanze del Garante per la protezione dei dati personali.

MISURE DA ADOTTARE NEI CONFRONTI DEGLI INCARICATI.

A) **Individuare**, tra i propri collaboratori, designandoli per iscritto, **gli Incaricati** del trattamento;

B) **recepire le istruzioni** cui devono attenersi gli Incaricati nel trattamento dei dati impartite dal Titolare, assicurandosi che vengano materialmente consegnate agli

stessi o siano già in loro possesso, unitamente al "**Regolamento per l'utilizzo dei servizi informatici aziendali**";

C) **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli incaricati del trattamento, curando in particolare il profilo della **riservatezza**, della **sicurezza di accesso** e della **integrità dei dati** e l'osservanza da parte degli Incaricati, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;

D) stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli Incaricati, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini del **riscontro** di eventuali richieste di esecuzione dei diritti di cui all'art. 7.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Una copia del presente atto di nomina dovrà essere restituita al Titolare, debitamente firmato per accettazione dal Azienda Sanitaria Locale n°8 - Cagliari, nella persona del suo legale rappresentante.

Il Direttore Generale Azienda AOU - Cagliari

_____

Il Legale Rappresentante Azienda Sanitaria Locale n°8 – Cagliari

_____

Data

Oggetto: Nomina a responsabile esterno per il trattamento dei dati relativi alla Videosorveglianza

IL DIRETTORE GENERALE

nella persona del legale rappresentante _____ della Azienda Ospedaliero Universitaria di Cagliari in qualità di Titolare del trattamento dei dati.

(D.lgs. 196/03):

- visto il Decreto Legislativo 30 giugno 2003, n. 196. "Codice in materia di protezione dei dati personali", di seguito definito "Codice";

- preso atto che l'art. 4, comma 1, lettera g) del suddetto Decreto definisce il "Responsabile" come la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali;

- atteso che l'art. 29, commi 2, 3, 4 e 5 del D. Lgs. n. 196/2003 dispone che: "*2. Se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. 3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione dei compiti. 4. I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare. 5. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni*";

- visto il D. lgs n. 82 del 7 marzo 2005 "Codice dell'amministrazione digitale";

- Considerato che, dalla lettura combinata dell'art. 37 del D.lgs. n. 196/03 e del comunicato stampa, esplicativo, pubblicato dall'Autorità Garante il 26 aprile 2004, i titolari coinvolti in attività di trattamento dati "relativi ad una banca dati" o "prestati per via telematica" ovvero "relativi alla fornitura di beni", devono procedere alla notificazione prima dell'inizio del trattamento.

- Considerato che la Ditta IMMA procede materialmente alla videosorveglianza dei locali del Presidio Ospedaliero Policlinico di Monserrato dell'AOU – Cagliari, con relativa registrazione di immagini.

Allegato 5

NOMINA

La Ditta IMMA nella persona del rappresentante legale _____ Responsabile del trattamento dei dati, effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi per l'esclusivo ambito di attività, attribuitegli, che ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le seguenti istruzioni impartite dal Titolare.

Compiti ed istruzioni per il Responsabile del Trattamento dei Dati Personali

in applicazione
del "Codice in materia di protezione dei dati personali" (D.Lgs.n. 196/2003)

9. PRINCIPI GENERALI DA OSSERVARE

Ogni *trattamento* di dati personali deve avvenire, nel rispetto dei seguenti **principi di ordine generale**:

Ai sensi dell'art. 11 del Codice, che prescrive le "*Modalità del trattamento e requisiti dei dati",* per ciascun trattamento di propria competenza, il Responsabile del Trattamento deve fare in modo che i dati siano trattati:

- secondo il principio di **liceità,** ossia conformemente alle disposizioni del Codice, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
- secondo il principio fondamentale di **correttezza**, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal **principio fondamentale di riservatezza** e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Codice è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

Ciascun **Responsabile** deve, inoltre, essere a conoscenza del fatto che per la violazione delle disposizioni in materia di trattamento dei dati personali sono previste **sanzioni penali** (artt. 167 e ss.).
In ogni caso la **responsabilità penale** per eventuale uso non corretto dei dati oggetto di tutela, resta a carico della singola persona cui l'uso illegittimo degli stessi sia imputabile.

Mentre, in merito alla **responsabilità civile,** si fa rinvio all'art. 15 del Codice, che dispone relativamente ai danni cagionati per effetto del trattamento ed ai conseguenti obblighi di risarcimento, implicando, a livello pratico, che, per evitare ogni responsabilità, l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire appunto la sicurezza dei dati detenuti.

10. COMPITI PARTICOLARI DEL RESPONSABILE

Il **Responsabile** del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti **compiti di carattere particolare**:

A) attenersi rigorosamente, per ciascun trattamento di dati personali e/o sensibili, al rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

B) definire, per ciascun trattamento di dati personali e/o sensibili, la **durata** del trattamento e la **cancellazione** o anonimizzazione dei dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

C) assicurare che la **comunicazione a terzi** e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali.

D) adempiere agli **obblighi di sicurezza**, quali:

E) adottare le **misure minime di sicurezza** espressamente previste dal Codice della Privacy. Tra queste ultime, in particolare, si segnala l'obbligo (lett. g – art. 34) di collaborare con il Titolare alla stesura e aggiornamento annuale del Documento Programmatico sulla Sicurezza (DPS), nelle modalità di volta in volta indicate.

F) **comunicare** tempestivamente al Titolare casi di **accesso non autorizzato** ai dati o di trattamento non consentito, o non conforme alle finalità istituzionali.

G) far osservare gli adempimenti previsti in caso di **nuovi trattamenti** e **cancellazione** di trattamenti*:*

H) in particolare, comunicare preventivamente al Titolare l'inizio di ogni attività (trattamento) che deve essere oggetto di notifica al Garante ex art. 37 del Codice;

I) segnalare al Titolare l'eventuale cessazione di trattamento.

J) collaborare con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal D. Lgs. 196/2003 e segnalare eventuali problemi applicativi.

K) trasmettere le richieste degli interessati al titolare, al fine di garantire l'esercizio dei diritti dell'interessato, ai sensi degli artt. 7, 8, 9 e 10 del D. Lgs. 196/2003.

L) collaborare con il Titolare per l'evasione delle richieste degli interessati ai sensi dell'art. 10 del D. Lgs. 196/2003 e delle istanze del Garante per la protezione dei dati personali.

MISURE DA ADOTTARE NEI CONFRONTI DEGLI INCARICATI.

A) **Individuare**, tra i propri collaboratori, designandoli per iscritto, **gli Incaricati** del trattamento;

B) **recepire le istruzioni** cui devono attenersi gli Incaricati nel trattamento dei dati impartite dal Titolare, assicurandosi che vengano materialmente consegnate agli stessi o siano già in loro possesso, unitamente al "**Regolamento per l'utilizzo dei servizi informatici aziendali**";

C) **adoperarsi** al fine di rendere effettive le suddette istruzioni cui devono attenersi gli incaricati del trattamento, curando in particolare il profilo della **riservatezza**, della **sicurezza di accesso** e della **integrità dei dati** e l'osservanza da parte degli Incaricati, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;

D) stabilire le modalità di **accesso** ai dati e l'organizzazione del lavoro degli Incaricati, avendo cura di adottare preventivamente le misure organizzative idonee e impartire le necessarie istruzioni ai fini del **riscontro** di eventuali richieste di esecuzione dei diritti di cui all'art. 7.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Una copia del presente atto di nomina dovrà essere restituita al Titolare, debitamente firmato per accettazione dalla Ditta IMMA , nella persona del suo legale rappresentante.

Il Direttore Generale Azienda AOU - Cagliari

_____

Il Legale Rappresentate Ditta IMMA – Cagliari

_____

Data

Allegato 7

Egr. Sig.

OGGETTO: consenso informato per i lavoratori dipendenti ai sensi dell'art. 13 del Decreto Legislativo 196/2003

La scrivente La informa che, per l'instaurazione e la gestione del rapporto di lavoro con Lei in corso, è titolare di dati Suoi e dei Suoi familiari qualificati come dati personali ai sensi del Codice in materia di protezione dei dati personali (D. Lgs. 196/2003).

La informiamo, pertanto, che tali dati verranno trattati con il supporto di mezzi cartacei, informatici o telematici per i seguenti fini:

l'elaborazione ed il pagamento della retribuzione;

l'adempimento degli obblighi, legali e contrattuali, anche collettivi, connessi al rapporto di lavoro;

Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità per l'azienda di dare esecuzione al contratto o di svolgere correttamente tutti gli adempimenti, quali quelli di natura retributiva, contributiva, fiscale e assicurativa, connessi al rapporto di lavoro.

In aggiunta alle comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati in Italia esclusivamente per le finalità sopra specificate a:

- Enti pubblici (INPDAP, INPS, INAIL, Uffici fiscali, ecc.);
- Fondi o Casse anche private di previdenza e assistenza;
- Studi medici o laboratori di analisi in adempimento degli obblighi in materia di igiene e sicurezza del lavoro;
- Società di assicurazioni;
- Istituti di credito;
- Organizzazioni sindacali cui lei abbia conferito specifico mandato;
- Fondi integrativi;
- Organizzazioni imprenditoriali cui aderisce l'azienda;
- Collegio Sindaci Revisori
- Enti pubblici e/o privati con cui l'Azienda abbia instaurato rapporti e convenzioni necessari per il raggiungimento dei propri scopi.

Relativamente ai dati medesimi potrete esercitare i diritti previsti dall'art. 7 del D.Lgs n. 196/2003 (di cui viene allegata copia) nei limiti ed alle condizioni previste dagli articolo 8, 9 e 10 del citato decreto legislativo.

In relazione al rapporto di lavoro, L'Azienda potrà trattare dati che la legge definisce "sensibili" in quanto idonei a rilevare ad esempio:

uno stato generale di salute (assenze per malattia, maternità, infortunio o l'avviamento obbligatorio) idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive/periodiche o richieste da Lei stesso/a);

l'adesione ad un sindacato (assunzione di cariche e/o richiesta di trattenute per quote di associazione sindacale), l'adesione ad un partito politico o la titolarità di cariche pubbliche elettive (permessi od aspettativa), convinzioni religiose (festività religiose fruibili per legge);

I dati di natura sensibile, concernenti lo stato di salute, che tratta il medico competente nell'espletamento dei compiti previsti dal D.Lgs. n. 81/2008 e ss.mm.ii. dalle altre disposizioni in materia di igiene e sicurezza nei luoghi di lavoro, per l'effettuazione degli accertamenti medici preventivi e periodici, verranno trattati presso il datore di lavoro esclusivamente dallo stesso medico quale autonomo titolare del trattamento, per il quale l'Azienda chiede espresso consenso. I soli giudizi sull'inidoneità verranno comunicati dal medico allo stesso datore di lavoro.

I dati personali non sono soggetti a diffusione.

Tutti i dati predetti e gli altri costituenti il Suo stato di servizio verranno conservati anche dopo la cessazione del rapporto di lavoro per l'espletamento di tutti gli eventuali adempimenti connessi o derivanti dalla conclusione del rapporto di lavoro stesso.

Titolare del trattamento dei Suoi dati personali è:
Prof. Pietro Paolo Murru

Responsabile del trattamento dei Suoi dati personali è:

Gli incaricati del trattamento dati sono

Responsabile del Trattamento dati

La preghiamo di restituirci datata e firmata, anche da parte dei suoi familiari maggiorenni, copia della presente come consenso espresso e ricevuta delle informazioni sopraesposte e del testo dell'art.7 del Decreto Legislativo 196/2003.

CONSENSO DEL LAVORATORE DIPENDENTE/COLLABORATORE

Il sottoscritto _____ Nato a _____
il _____ C.F. _____

dichiara

di aver ricevuto dal Responsabile del trattamento dei dati dell'A.O.U. di Cagliari, completa informativa ai sensi dell'art. 13 del D. Lgs. N° 196/2003, unitamente a copia dell'art. 7 del decreto medesimo ed esprime il suo libero e spontaneo consenso al trattamento ed alla comunicazione dei propri dati personali conferiti alla predetta Azienda, con particolare riguardo a quelli definiti "sensibili" dall'art. 4, comma 1, lettera d), del D. Lgs. N° 196/2003, nei limiti, per le finalità e per la durata precisati nell'informativa.

Data,

Il Lavoratore/Collaboratore

_____
(firma per esteso)

Art. 7 Dlgs 196/2003 - Diritto di accesso ai dati personali ed altri diritti -

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Allegato 8

AZIENDA OSPEDALIERO UNIVERSITARIA DI CAGLIARI:

INFORMATIVA AGLI UTENTI SUL TRATTAMENTO DEI DATI PERSONALI (ART. 13, D.Lgs30.6.2003 N° 196 CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI)

Ai sensi della norma in epigrafe, si informa che il trattamento dei dati personali, anche di natura sensibile, raccolti presso le strutture sanitarie dell'Azienda Ospedaliero Universitaria Di Cagliari è finalizzato:

- ✓ alla tutela della salute e dell'incolumità fisica dell'interessato;
- ✓ alla tutela dell'incolumità fisica di terzi e della collettività;
- ✓ alla ricerca scientifico-statistica ed epidemiologica, finalizzata alla tutela della salute ed incolumità fisica dell'interessato di terzi e della collettività;
- ✓ allo svolgimento dei compiti del Servizio Sanitario Nazionale annoverati tra le finalità di rilevante interesse pubblico dall'art. 85 del D.Lgs 196/2003, vale a dire:
  - attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale;
  - programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
  - vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
  - attività certificatorie;
  - attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;
  - instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.

Per lo svolgimento delle attività istituzionali previste dall'ordinamento del Servizio Sanitario Nazionale, e in base alla natura delle prestazioni richieste, i dati personali raccolti comprendono dati sensibili, nella fattispecie dati idonei a rivelare lo stato di salute e la vita sessuale, nonché di dati genetici e di taluni dati biometrici; nei casi e con i limiti previsti dalle normative settoriali vigenti tali dati sono altresì effettuati trattamenti di dati personali e sensibili per la rilevazione delle malattie mentali, delle malattie infettive e diffusive e della sieropositività, a fini di indagini epidemiologiche a fini di trapianto di organi e tessuti, o a fini di monitoraggio della spesa sanitaria.

Si informa inoltre che all'interno dell'Azienda Ospedaliero Universitaria sono in funzione videocamere a circuito chiuso, per esclusivi motivi di sicurezza e sorveglianza da attività illecite. Le immagini eventualmente raccolte sono trattate nel rispetto delle prescrizioni di cui all'art. 11 del D.Lgs. 196/2003 e di ogni eventuale prescrizione specifica dell'Autorità Garante.

Il trattamento dei dati personali avverrà nel rispetto del segreto professionale, del segreto d'ufficio e dei principi di correttezza, liceità e trasparenza, in applicazione di quanto disposto dalla normativa vigente, in modo da assicurare la tutela della riservatezza e dei diritti dell'utente e degli altri interessati. Per tutti i trattamenti potranno essere utilizzati anche sistemi informatici e telematici.

L'eventuale utilizzazione dei dati personali per fini di ricerca scientifica o statistica avverrà soltanto con il consenso dell'interessato, prestato con le modalità di cui all'art. 81 del D.Lgs.n.196/2003 o solo dopo che i dati stessi saranno stati resi anonimi.

Si precisa che per l'assolvimento dei compiti istituzionali, in conformità alle disposizioni di Legge o di regolamento in materia, i dati relativi alle prestazioni erogate sono regolarmente trasmessi alla Regione Sardegna, alle Aziende U.S.L. di appartenenza dell'utente interessato; per le attività di rispettiva competenza istituzionale al Ministero della Salute ed in generale agli Enti del SSN; potrà aversi comunicazione di dati ad altri enti o aziende della Pubblica Amministrazione nazionale, quando questi ne abbiano fatto legittima richiesta per l'espletamento dei rispettivi compiti istituzionali.
La comunicazione dei dati ad altri soggetti pubblici verrà effettuata in esecuzione di obblighi normativi o per lo svolgimento delle funzioni istituzionali, previa comunicazione al Garante per la protezione dei dati personali. La comunicazione a soggetti privati sarà effettuata solo nei casi previsti da norme di legge o di regolamento. Non verrà effettuata alcuna diffusione dei dati idonei a rivelare lo stato di salute, ai sensi dell'art. 22, comma 8 del D.Lgs.n.196/2003.

Il **titolare** del trattamento dei dati personali è: **Azienda Ospedaliero Universitaria Di Cagliari, Via Ospedale 54 Cagliari ,** nella persona fisica del proprio legale rappresentante, il Direttore Generale

Sono individuati quali **responsabili** del trattamento dei dati personali i Direttori o i Dirigenti Responsabili delle strutture operative dell'Azienda (Unità Operative, Sezioni, Uffici) presso le quali i trattamenti sono effettuati. I nominativi dei responsabili possono essere richiesti in ogni momento all'U.O. Affari Generali dell'Azienda Ospedaliero Universitaria di Cagliari.

Le funzioni di **incaricato** al trattamento di dati personali sono svolte, secondo la graduazione di funzioni e di responsabilità professionali previste per ogni figura dalla normativa vigente, da:
- personale sanitario dirigente del SSN (medico, biologo, farmacista, chimico) o universitario, appartenente alla Facoltà di Medicina o Chirurgia dell'Università degli Studi di Cagliari
- personale professionale (infermieristico e tecnico sanitario)
- personale ausiliario di assistenza e, in taluni casi, personale ausiliario economale
- personale dei ruoli tecnico e amministrativo del SSN

In alcuni casi e previa specifica autorizzazione potranno inoltre essere incaricati del trattamento: medici specializzandi universitari, ricercatori universitari, studenti del triennio di formazione clinica della Facoltà di Medicina o Chirurgia dell'Università degli Studi di Cagliari.

L'utente potrà rivolgere istanza per far valere i propri diritti, **ai sensi dell'art. 7 del Decr. Legislativo 196/2003**, di sotto riportati per estratto, presso l'U.O. Affari Generali Azienda Ospedaliero Universitaria di Cagliari Via Ospedale 54 Cagliari

Il Titolare del trattamento dati

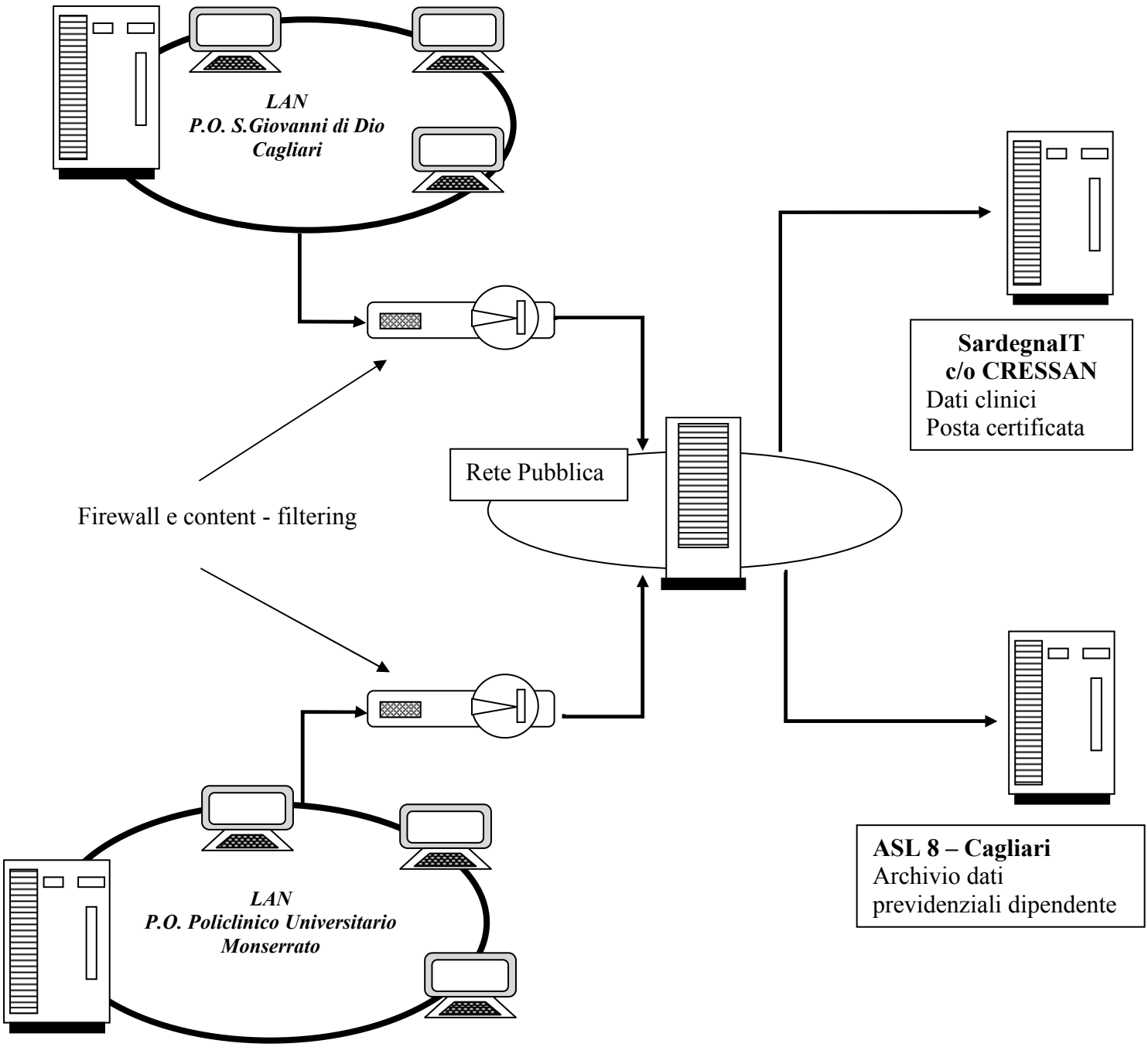
( )

Art. 7 (estratto) - Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art. 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi, in tutto o in parte: per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo de

Schema 1: LAN AOU - Cagliari



Dichiarazione di impegno

Il presente Documento Programmatico sulla Sicurezza è approvato, adottato e firmato dal Direttore Generale in qualità di Titolare del trattamento dei dati. Esso verrà aggiornato periodicamente entro il 31 Marzo di ogni anno.

La versione originale del Documento è custodita presso la sede legale dell'Azienda Ospedaliera Universitaria di Cagliari , così come indicato nei Riferimenti dell'Azienda sul frontespizio del presente documento , per essere esibita in caso di controllo.

Una copia cartacea o su supporto elettronico verrà consegnata ai responsabili dei trattamento dei dati, al fine di diffonderne i contenuti agli aventi diritto.

Cagliari _____

Il Direttore Generale – Titolare t.d.