

AZIENDA OSPEDALIERA  
FATEBENEFRAPELLI E OFTALMICO  
MILANO



Presidio Ospedaliero Fatebenefratelli e Oftalmico  
Presidio Ospedaliero Macedonio Melloni

# **DOCUMENTO PROGRAMMATICO SULLA SICUREZZA AZIENDALE**

**(art. 34 del Codice in materia di protezione dei dati personali e regola 19,  
Allegato B, del D.lgs. n. 196/2003)**

---

Corso di Porta Nuova n. 23 – 20121 Milano – tel. 02.6363.1

## 1. PREMESSA

L'Azienda Ospedaliera Fatebenefratelli e Oftalmico è un organismo sanitario pubblico di alta specializzazione che si caratterizza per la sua attività polispecialistica, di emergenza-urgenza e di concreta integrazione con il territorio. L'Azienda ospedaliera intende adempiere alla propria "missione" con efficacia ed efficienza e vuole perseguire la centralità del paziente che, assieme alla professionalità degli operatori, è la vera guida del "sistema qualità". L'attività strategica e operativa si basa su indirizzi che mirano:

- al miglioramento continuo della qualità, che corrisponde alla capacità di soddisfare le legittime esigenze e le aspettative di tutte le parti interessate: cittadini, pazienti, regione, enti locali, operatori, medici di medicina generale, fornitori di beni e servizi;
- alla gestione, quale strumento per il raggiungimento degli obiettivi fissati dal piano strategico e di sviluppo.

Nell'utilizzo degli strumenti gestionali l'Azienda è soggetta al rispetto delle attività di tutela del cittadino che sono guidate da principi di: etica, uguaglianza, imparzialità, qualità e appropriatezza delle prestazioni, diritto di scelta, efficienza, partecipazione, diritti del malato e sono garantite da rispetto della dignità della persona, diritto alla differenza senza preclusioni di età, sesso, nazionalità, cultura e religione, corretta informazione sull'utilizzo dei servizi, rispetto della Privacy. I servizi offerti dall'Azienda Ospedaliera sono comprensivi di azioni o prestazioni di diagnosi, cura, riabilitazione e assistenza, necessarie per risolvere i problemi di salute dell'utente e sono articolati secondo modelli organizzativi riferiti alle attività di urgenza, di ricovero programmato e ambulatoriali. L'effettiva tutela dei diritti degli utenti, sancita dai principi sopra ricordati, è garantita anche dalla presenza di strumenti a disposizione dei cittadini; in particolare l'Azienda Ospedaliera riconosce al cittadino la possibilità di controllo della qualità dei servizi erogati, che può essere esercitato individualmente, ovvero dalle Associazioni di tutela dei malati, dal volontariato e con mezzi di comunicazione. Al fine di offrire strumenti di valutazione, l'Azienda è impegnata nell'approntare e pubblicizzare adeguatamente standards quanti-qualitativi circa le modalità di erogazione dei servizi offerti. La qualità del servizio sanitario viene garantita dalla capacità professionale di risposta ai bisogni di salute del cittadino, dai tempi e dalla semplicità delle

procedure di accesso, dall'informazione, orientamento, accoglienza, comfort e pulizia, nonché dalle relazioni umane e sociali.

La struttura dell'Azienda ospedaliera è costituita da:

- Ospedale Fatebenefratelli e Oftalmico, Ospedale Macedonio Melloni
- Uonpia (via stefanardo, via sant'erlembardo, corso plebisciti, via pusiano)
- Cps (via settembrini, via betti, via pusiano, via procaccini)
- Cd (via pusiano, via settembrini)

L'organizzazione dell'Azienda ospedaliera contempla

- Direzione generale, Direzione amministrativa, Direzione sanitaria
- Collegio di Direzione
- Uffici di staff alla Direzione generale
- Dipartimenti sanitari
- Dipartimento amministrativo
- Consiglio dei sanitari

Premesso tutto ciò, e vista la normativa in materia di trattamento di dati personali ed in particolare il Decreto legislativo 30 giugno 2003 n. 196; l'Allegato B) o Disciplinare tecnico in materia di misure minime di sicurezza; il Regolamento della Regione Lombardia n. 9 del 18 luglio 2006 per il trattamento dei dati sensibili e giudiziari; i Provvedimenti dell'Autorità Garante per la Protezione dei dati personali; al fine di ottemperare alla normativa citata l'Azienda Ospedaliera Fatebenefratelli e Oftalmico quale Titolare del trattamento dati aggiorna il presente

### **Documento Programmatico sulla Sicurezza (DPS)**

che definisce la Politica aziendale in materia di Privacy e le misure approntate dall'Azienda Ospedaliera medesima per garantire il livello minimo di sicurezza nel trattamento dei dati personali.

Il DPS, da custodirsi presso la sede dell'Azienda, deve essere oggetto di rinnovo entro il 31 marzo di ogni anno. Il presente documento deve essere conosciuto ed applicato dal Titolare, dai Responsabili e dagli Incaricati nominati, ciascuno secondo le proprie responsabilità e competenze.

## **2. PUNTI PRINCIPALI DEL DOCUMENTO**

Nel presente Documento programmatico sono indicati i punti previsti dal paragrafo 19 del Disciplinare tecnico (ovvero l'Allegato B al Codice), argomenti ai quali si aggiungono i punti relativi alla sicurezza del documento cartaceo, all'adozione delle misure di garanzia e all'attività di monitoraggio svolta:

- elenco trattamenti dati personali (regola 19.1 Allegato b)
- distribuzione dei compiti e delle responsabilità (regola 19.2 Allegato b)
- amministratore di sistema
- analisi dei rischi che incombono sui dati (regola 19.3 Allegato b)
- misure in essere e da adottare (regola 19.4 Allegato b)
- criteri e modalità di ripristino della disponibilità dei dati (regola 19.5 Allegato b)
- pianificazione degli interventi formativi previsti (regola 19.6 Allegato b)
- trattamenti affidati all'esterno (regola 19.7 Allegato b)
- separazione dei dati (regola 19.8 Allegato b)
- progetto crs-siss
- aggiornamento

### **3. ELENCO DEI TRATTAMENTI DI DATI PERSONALI (regola 19.1 del Disciplinare)**

In questa sezione sono individuati i trattamenti effettuati dal Titolare, direttamente o attraverso collaborazioni esterne. Il trattamento dei dati avviene nel rispetto dei diritti e delle libertà fondamentali dell'interessato ed è compiuto quando, per lo svolgimento delle finalità di interesse pubblico perseguite, non è possibile il trattamento dei dati anonimi oppure di dati personali non sensibili o giudiziari (art. 2, Regolamento regionale del 18 luglio 2006 n. 9). I dati sono ripartiti per natura di appartenenza come di seguito indicato:

#### Dati personali

I dati personali sono costituiti da 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 e le foto scattate ai fini di interventi chirurgici, secondo quanto chiarito dall'Autorità Garante per la protezione dei dati personali. Nello specifico trattasi di dati relativi a persone fisiche e persone giuridiche in rapporto con l'Azienda Ospedaliera ovvero pazienti, personale dipendente, personale non strutturato (borsisti, collaboratori, tirocinanti), terzi fornitori, trattati attraverso le strutture sanitarie e amministrative preposte, come meglio indicato nella parte dedicata all'elenco delle strutture (v. *infra* pagina 10).

#### Dati sensibili

I dati sensibili sono quei particolari dati personali idonei a rilevare 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, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale. Nella fattispecie trattasi di dati contenuti in cartelle cliniche di ricovero, diari clinici, registri delle prenotazioni, relazioni cliniche di dimissioni dirette al medico di famiglia, archivi di attività diagnostiche/terapeutiche svolte per i pazienti ricoverati, registri di sala operatoria, registri delle trasfusioni, registri e documenti relativi alle sperimentazioni cliniche, raccolte di dati con finalità amministrativo-contabili, raccolte di dati relativi a esposti (lamentele, opinioni) degli utenti, trattati attraverso le strutture sanitarie e

amministrative preposte, come meglio indicato nella parte dedicata all'elenco delle strutture (v. *infra* pagina 10).

Nella redazione delle liste trattamenti si è altresì tenuto conto delle informazioni contenute nella notificazione inviata al Garante in data 30 aprile 2004. Tale notifica è rintracciabile in via telematica, attraverso il sito della predetta Autorità, nell'apposito Registro Pubblico all'indirizzo <http://www.garanteprivacy.it> al quale si rinvia. I dati sensibili e giudiziari oggetto di trattamento, le finalità di interesse pubblico perseguite, nonché le operazioni eseguibili sono individuati conformemente alle schede contenute nell'Allegato B al regolamento regionale citato (art. 3). Le tabelle che sono state compilate hanno ad oggetto:

tabella 1: trattamento di dati genetici come meglio precisato: dati idonei a rivelare patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali; dati idonei a rivelare la gravità o il decorso del quadro clinico delle patologie genetiche, dati idonei a identificare malattie ereditarie; dati relativi a indagini epidemiologiche; dati relativi a indagini sulla popolazione; dati relativi a trapianti di tessuti od organi o all'impiego di cellule staminali; dati relativi alla procreazione. Dette categorie di dati sono trattati per perseguire finalità di prevenzione di determinate patologie; cura e terapia degli interessati; programmi terapeutici o di prevenzione; diagnosi delle patologie genetiche (test diagnostici); diagnosi di patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali; screening neonatali; sperimentazioni farmacologiche ad uso clinico; trapianti di organi e tessuti.

tabella 4: trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria come meglio precisato: dai idonei a rivelare l'identità del donatore; dati idonei a rivelare l'identità del ricevente, dati idonei a rivelare la vita sessuale; dati idonei a rivelare lo stato di disabilità; dati idonei a rivelare sieropositività; dati idonei a rivelare malattie infettive e diffuse, dati idonei a rivelare malattie mentali; dati idonei a rivelare stato di salute; dati a relativi indagini epidemiologiche; dati relativi a prescrizioni farmaceutiche e cliniche; dati relativi ad esiti diagnostici e programmi terapeutici; dati relativi all'utilizzo di particolari ausili protesici; dati relativi alla prenotazione di esami clinici e visite specialistiche; dati idonei a rivelare lo stato di aids conclamato.

Dette categorie di dati sono trattati per perseguire finalità di assistenza sanitaria; trapianto di organi e tessuti; attività di teleconsulto, telediagnosi o telemedicina; diagnosi, cura o terapia dei pazienti; gestione amministrativa; indagine epidemiologica; prevenzione di patologie genetiche in popolazioni a rischio; prenotazione e refertazione esami clinici o visite specialistiche per via telematica o telefonica; procreazione assistita; registrazione dei pazienti; ricerca medica o biomedica; rilevazione di malattie infettive e diffuse; rilevazione di malattie mentali; rilevazione di stati di sieropositività; schede cliniche informatizzate.

### Dati giudiziari

I dati giudiziari sono quei particolari dati personali idonei a rivelare 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 di indagato ai sensi degli art. 60 e 61 del codice di procedura penale. Nello specifico può trattarsi di dati giudiziari relativi al detenuto ricoverato per prestazioni di tipo ospedaliero.

### Trattamenti correlati al SISS

L'Azienda ospedaliera svolge inoltre le operazioni di trattamento come identificate nel Progetto SISS e di seguito indicate:

- l'Azienda ospedaliera relativamente a trattamenti per finalità amministrative, è Titolare dei trattamenti di registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, interconnessione, raffronto, utilizzo e comunicazione relativi a prescrizioni, prenotazioni, erogazioni, eventi sanitari, esenzioni, flussi di rendicontazione e anagrafica;
- l'Azienda ospedaliera relativamente a trattamenti per finalità di cura, è Titolare dei trattamenti di registrazione, conservazione, elaborazione, selezione, estrazione, interconnessione, raffronto e comunicazione relativi alla gestione delle basi dati inerenti all'utilizzo del Fascicolo Sanitario Elettronico (FSE) e del consenso.

### Tipologia delle operazioni eseguite

I dati come sopra indicati sono oggetto di operazioni di trattamento standard e particolari come di seguito indicate: raccolta dati forniti dall'interessato, forniti da soggetto privato diverso dall'interessato, forniti da soggetto pubblico; la registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione. Interconnessione e raffronti con altri trattamenti o archivi della stessa azienda ospedaliera; comunicazione da parte dell'azienda ospedaliera verso soggetti pubblici, verso l'Azienda sanitaria di residenza dell'interessato (qualora diversa), verso la Regione.

### Operazioni di trattamento particolari: Videosorveglianza ai fini di sicurezza e tutela del patrimonio aziendale

Presso l'Azienda Ospedaliera Fatebenefratelli e Oftalmico sono attivi due sistemi di videosorveglianza che permettono la ripresa e la registrazione di immagini per le seguenti finalità:

1. sicurezza delle persone;
2. tutela del patrimonio;
3. controllo di aree comuni.

Per i sistemi di cui trattasi è esclusa ogni finalità che possa essere ricondotta al controllo a distanza dei lavoratori, alla cura dei pazienti ed alla raccolta di immagini idonee a rivelare lo stato di salute degli stessi. Per mezzo dei sistemi non è quindi operato alcun controllo di ambienti nei quali sia svolta attività sanitaria su pazienti.

L'Azienda ha provveduto a nominare il Responsabile dei sistemi di videosorveglianza ed i soggetti incaricati ad accedere alle immagini, nel rispetto delle vigenti disposizioni in materia di protezione dei dati personali e con l'adozione delle misure minime di sicurezza. Nel perseguire le tre finalità sopra richiamate l'azienda ha adottato il "REGOLAMENTO PER LA GESTIONE DEI SISTEMI DI VIDEOSORVEGLIANZA DELL'A.O. FATEBENEFRATELLI E OFTALMICO". Tale regolamento, allegato 1, costituisce parte integrante e sostanziale del presente DPS ed è reso consultabile mediante pubblicazione sui siti internet e intranet aziendali.

I dati personali, rappresentati dalle immagini acquisite, vengono trattati e conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali gli stessi sono stati raccolti e/o successivamente trattati.

La cancellazione automatica da ogni supporto informatico avviene mediante sovraregistrazione con modalità tali da rendere non riutilizzabili i dati cancellati. I sistemi provvedono alla cancellazione automatica delle registrazioni trascorso il termine fissato per la loro conservazione nel citato regolamento ( vedi allegato 1).

Per quanto concerne l'obbligo di informativa di cui all'art. 13 del codice privacy, i modelli utilizzati sono contenuti nel sopra citato regolamento.

#### Adempimento obblighi di informativa e consenso

Rispetto al trattamento delle sopraindicate tipologie di dati in tutte le strutture ospedaliere e territoriali sono in uso un modello di informativa ed un modello di acquisizione del consenso per il trattamento dei dati, predisposti in conformità alle indicazioni di cui agli articoli 76 e seguenti del codice privacy. Tali modelli sono altresì reperibili, in uno spazio dedicato alla materia, nella intranet aziendale.

In particolare:

- l' informativa per il trattamento dati dei pazienti/assistiti è affissa in modo da essere visibile dal soggetto interessato al quale i dati si riferiscono (sale d'attesa, punti accettazione, reparti)
- il modello di consenso è trasmesso al soggetto interessato e fatto firmare allo stesso oppure o a chi lo rappresenta, nell'ipotesi di ricovero programmato. Per quanto concerne le prestazioni ambulatoriali è attiva un'apposita casella denominata "consenso privacy" che, flaggata dall'operatore sanitario all'atto dell'accettazione in Ospedale, consente di adempiere all'obbligo in questione attraverso la modalità semplificata contemplata dal codice privacy all'articolo 81.

#### Elenco delle specialità e degli ambulatori

Le informazioni come sopra rappresentate sono oggetto di trattamento nelle strutture aziendali, ripartite in specialità e ambulatori, come indicate nel sito [www.fbf.milano.it](http://www.fbf.milano.it).

#### **4. DISTRIBUZIONE DI COMPITI E RESPONSABILITÀ (regola 19.2 Disciplinare tecnico)**

##### Il Titolare del trattamento

Il Titolare del trattamento dei dati è l'Azienda Ospedaliera Fatebenefratelli e Oftalmico nella persona del suo Rappresentante Legale, cui competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento ha esercitato la facoltà di nominare i Responsabili del trattamento dei dati ed affidare loro, per quanto di competenza, il compito di porre in essere ogni misura tesa a ridurre al minimo i rischi di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previa idonee istruzioni.

##### I Responsabili del trattamento

I Responsabili del trattamento sono stati individuati fra i dirigenti delle strutture sanitarie e amministrative 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.

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 sopra e delle proprie istruzioni. Si è provveduto ad effettuare la nomina dei soggetti Responsabili del trattamento a mezzo apposito modello predisposto dalla società di consulenza, trasmesso e fatto firmare ai Responsabili così nominati. Nelle pagine seguenti sono rispettivamente riportati i modelli di lettera con i quali si sono nominati i Responsabili e le istruzioni per gli stessi:

## **NOMINA DEL RESPONSABILE INTERNO TRATTAMENTO DATI**

*Al Sig.*

*Dott.*

*Direttore/Dirigente*

*U.O./Struttura*

*SEDE*

*Oggetto: Nomina a "Responsabile" del trattamento dati.*

*Si comunica che con deliberazione n. \_\_\_\_\_ del \_\_\_\_\_, il Direttore Generale, in qualità di legale rappresentante di questa Azienda, l'ha nominata "Responsabile" del trattamento dei dati personali relativi alle banche dati e agli archivi gestiti nell'ambito della U.O./Struttura da Lei diretta, conformemente a quanto stabilito dall'art. 29 D.Lgs. n. 196/03 (Codice Privacy).*

*Si allegano le istruzioni relative ai principali adempimenti ai quali è tenuto il Responsabile del trattamento, con invito a trasmettere copia della presente, debitamente sottoscritta, alla U.O. Affari generali e Legali (Fax n. 2417).*

*Con i più cordiali saluti.*

*Il Direttore Amministrativo*

## **ISTRUZIONI PER IL RESPONSABILE INTERNO**

*L'Azienda ospedaliera "Fatebenefratelli e Oftalmico", in qualità di Titolare del trattamento dati, in attuazione a quanto stabilito dall'art. 29 D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) impartisce al Responsabile interno le istruzioni come di seguito specificate:*

- 1. trattare i dati personali esclusivamente per lo svolgimento di finalità istituzionali, nei limiti e con le modalità stabilite dalla normativa vigente e dalle istruzioni impartite dal Titolare;*
- 2. verificare periodicamente l'esattezza, la pertinenza, la completezza, la non eccedenza dei dati trattati rispetto alle finalità perseguite e provvedere, quando necessario, al loro aggiornamento;*
- 3. collaborare con il Titolare nel monitoraggio degli adempimenti privacy con particolare riferimento all'aggiornamento dell'elenco dei trattamenti, alla predisposizione del Documento programmatico e all'adozione delle misure di sicurezza;*
- 4. adottare le modalità idonee ad assicurare al soggetto interessato l'esercizio dei propri diritti ai sensi dell'art. 7 del citato decreto;*
- 5. nominare i propri collaboratori che svolgono operazioni di trattamento dati quali "Incaricati" mediante l'apposito modello aziendale e definire l'ambito di trattamento al quale i medesimi possono accedere;*
- 6. informare il paziente in merito alle caratteristiche del trattamento mediante affissione del modulo "Informativa sul trattamento dati" in luogo accessibile dall'utenza;*
- 7. acquisire il consenso al trattamento dati del paziente mediante compilazione del modulo "Consenso al trattamento dati" e conservare il medesimo in cartella clinica;*
- 8. definire le istruzioni alle quali i medesimi Incaricati devono attenersi nello svolgimento di operazioni di trattamento dati su supporto cartaceo;*
- 9. definire le istruzioni alle quali i medesimi Incaricati devono attenersi nello svolgimento di operazioni di trattamento dati su supporto elettronico;;*
- 10. attenersi alle istruzioni impartite dal sottoscritto Titolare il quale, anche tramite verifiche ispettive periodiche, vigila sulla puntuale osservanza delle proprie istruzioni.*

### Gli Incaricati del trattamento

Le operazioni di trattamento possono essere effettuate solo da Incaricati che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite dai medesimi.

L'Azienda ospedaliera ha adempiuto all'obbligo di nomina ai sensi dell'art. 30, mediante designazione effettuata per iscritto e mediante individuazione puntuale dell'ambito del trattamento consentito. In particolare, ogni singola Unità Operativa ha provveduto, tramite apposito modello, a definire gli ambiti di trattamento consentiti a ciascuna categoria di incaricati nonché a renderli conoscibili agli incaricati medesimi.

La matrice di tale modello è reperibile in uno spazio dedicato alla materia, nella intranet aziendale.

## **5. AMMINISTRATORE DI SISTEMA**

Di seguito, con riferimento al provvedimento dell'Autorità Garante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (Provvedimento Garante Privacy del 27 novembre 2008 pubblicato sulla G.U. n. 300 del 24 dicembre 2008) si evidenzia quanto segue:

### Valutazione delle caratteristiche soggettive

L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Anche quando le funzioni di amministratore di sistema o assimilate sono attribuite solo nel quadro di una designazione quale incaricato del trattamento ai sensi dell'art. 30 del Codice, l'Azienda si attiene comunque a criteri di valutazione equipollenti a quelli richiesti per la designazione dei responsabili ai sensi dell'art. 29.

### Designazioni individuali

La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

### Elenco degli amministratori di sistema

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, sono riportati nei documenti interni aziendali.

### Verifica delle attività

L'operato degli amministratori di sistema sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare del trattamento, in modo da controllare la sua rispondenza alle

misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

### Registrazione degli accessi

L'Azienda Ospedaliera ha implementato una soluzione informatica finalizzata alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema (***Sistema di Log management per la conservazione degli accessi ai sistemi da parte degli utenti amministratori***), così come richiesto dal Provvedimento 27 novembre 2008.

La soluzione implementata si basa su un sistema informatico realizzato in ambiente open source che registra gli eventi legati alle utenze amministrative dei sistemi considerati.

Gli eventi, in tempo reale, vengono inviati ad un collettore di log centralizzato dove vengono conservati nel rispetto dei requisiti di completezza, inalterabilità e integrità per un periodo non inferiore a sei mesi.

Le caratteristiche tecniche sono descritte nel documento di progetto disponibile presso il Sistema Informativo Aziendale (Sistema di log management – Manuale di amministrazione).

## **6. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (regola 19.4 Disciplinare tecnico)**

Si rinvia all'apposito Allegato 2 al predetto Documento programmatico sulla sicurezza.

## **7. MISURE IN ESSERE E DA ADOTTARE (regola 19.4 Disciplinare tecnico)**

In tale sezione sono sinteticamente riportate le misure in essere e da adottare per contrastare i rischi individuati. Per misure si intendono gli strumenti di natura tecnica e organizzativa, così come le attività di verifica e controllo finalizzate ad assicurare l'efficacia delle stesse. Di seguito sono indicate le misure di sicurezza per il dato trattato senza mezzi elettronici e le misure di garanzia specifiche per strutture sanitarie. Per le misure di sicurezza relative al dato trattato con mezzi elettronici si rinvia all'apposito capitolo dell'Analisi IT.

### **Misure di sicurezza per il dato trattato senza mezzi elettronici**

Archivio corrente: quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli Incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate. A tal fine si possono utilizzare contenitori (armadi, schedari eccetera) oppure le stesse stanze ove la documentazione è riposta (da interpretarsi estensivamente quali "contenitori"), purché muniti di serratura tale da consentire un'effettiva selezione degli accessi a favore dei soli medici, infermieri e amministrativi (o altri soggetti autorizzati) del reparto. La chiusura a chiave del contenitore (o della stanza) dove si custodiscono i documenti recanti dati sensibili è consigliabile nell'ipotesi in cui lo stesso non sia direttamente controllato dal personale autorizzato (ovvero alla fine della giornata lavorativa, in pausa eccetera) e sia pertanto più elevato il rischio di perdita, di alterazione o di accesso non autorizzato ai dati.

Archivio storico: l'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate, registrate e preventivamente autorizzate. Il controllo accessi agli Archivi storici deve essere attuato a mezzo registro cartaceo da compilare nell'ipotesi di ingresso in archivio dopo l'orario di chiusura, al fine di limitare il rischio di accesso non autorizzato ai dati o di alterazione degli stessi.

Consegna: ogni consegna di atti e documenti deve sempre avvenire nel rispetto di misure minime di sicurezza. In particolare la consegna di atti e documenti contenenti dati personali dovrà sempre avvenire in busta chiusa e sigillabile all'interessato o delegato per iscritto al fine di ridurre al minimo la possibilità che soggetti terzi non autorizzati possano venire a conoscenza del contenuto.

Segreto professionale: non parlare né comunicare dati personali e/o sensibili riferiti a soggetti terzi per telefono o attraverso altri strumenti di comunicazione a distanza se non si è rigorosamente certi dell'identità del destinatario (Interessati o altra persona da questi autorizzata).

Accesso ai locali: tutto il personale che deve avere accesso ai dati personali per l'espletamento delle proprie funzioni, viene espressamente nominato per iscritto Incaricato del trattamento da parte del Responsabile interno del trattamento.

Istruzioni: gli Incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni formalizzate del Titolare o del Responsabile interno.

Distruzione: i dati che, a seguito delle verifiche sull'essenzialità del trattamento rispetto alle finalità perseguite, risultano eccedenti o non pertinenti o non necessari non possono essere più trattati, salvo che per l'eventuale conservazione, secondo le norme di legge, del documento che li contiene. Ciascun Responsabile deve, quindi, vigilare sulla correttezza del trattamento in particolare eliminando informazioni non direttamente riconducibili alle finalità del trattamento e interrompendo trattamenti non direttamente riconducibili alle finalità del trattamento.

### **Misure di garanzia**

Dignità dell'Interessati: La prestazione medica e ogni operazione di trattamento dei dati personali deve avvenire nel pieno rispetto della dignità dell'Interessati, dignità che 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. Nei reparti di rianimazione dove si possono visitare i degenti solo attraverso vetrate o

videoterminali sono adottati accorgimenti anche provvisori che delimitino la visibilità dell'Interessati durante l'orario di visita ai soli familiari e conoscenti. E' stato predisposto il documento recante le linee guida che gli studenti devono rispettare nell'accedere alle strutture ospedaliere.

Riservatezza nei colloqui e nelle prestazioni sanitarie: è doveroso adottare idonee cautele in relazione allo svolgimento di colloqui specie con il personale sanitario per evitare che in tali occasioni le informazioni sulla salute dell'Interessati 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.

Notizie su prestazioni di pronto soccorso: La notizia o la conferma circa una prestazione di pronto soccorso sono 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 - è preventivamente informato dall'organismo sanitario 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'Interessati.

Dislocazione dei pazienti nei reparti: L'Interessato cosciente e capace deve essere informato e posto in condizione di fornire all'atto del ricovero 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. In adempimento a ciò il modulo di consenso prevede che il paziente possa barrare la relativa opzione finalizzata ad un ricovero "in forma anonima". Possono essere fornite informazioni sullo stato di salute a soggetti diversi dall'Interessati 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'Interessati.

Distanza di cortesia: Nelle grandi sale d'attesa sono previste o in fase di attuazione le distanze di cortesia tra utente in fila e utente allo sportello, con l'ausilio di cartelli atti a sensibilizzare l'utenza al riguardo.

Ordine di precedenza e di chiamata: Nelle grandi sale d'attesa, nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa, devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli Interessati che prescindano dalla loro individuazione nominativa. 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 possono essere utilizzati altri accorgimenti adeguati ed equivalenti.

Correlazione fra paziente e reparto o struttura: Nella formazione del personale è prevista l'adozione di modalità finalizzate a 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. Analoghe garanzie sono adottate 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.

Regole di condotta per gli Incaricati: L'Azienda designa quali Incaricati o 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, al pari del personale medico ed infermieristico, gli altri soggetti che non sono tenuti per legge al segreto professionale sono 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, 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'Interessati: Le informazioni sullo stato di salute sono comunicate solo per il tramite di un medico autorizzato o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente.

Il personale designato è istruito debitamente anche in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'Interessati. 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.

### **Attività di verifica e controllo**

L'Azienda ospedaliera ha da tempo intrapreso un percorso di adeguamento normativo alle numerose e complesse prescrizioni del Codice Privacy e ai Provvedimenti emessi dall'Autorità Garante. In particolare si è pianificata, in collaborazione con apposita società di consulenza, un'attività di *audit* interno basata sulla elaborazione di un "Progetto Privacy" strutturato in modo tale da consentire lo svolgimento di tre attività di monitoraggio considerate fondamentali:

- attività formale: si è predisposta la "Cartella Privacy" contenente la modulistica e le procedure necessarie per l'adeguamento normativo delle strutture aziendali. La cartella è stata trasmessa al referente di struttura (Primario o Caposala a seconda della disponibilità), al quale sono stati illustrati la funzione e le modalità di applicazione dei singoli documenti.
- attività operativa: si sono svolti accessi *in loco* finalizzati a rilevare, mediante compilazione di apposita *check list*, l'esistenza di eventuali criticità privacy (di tipo logistico, organizzativo o tecnologico) e consentire quindi la predisposizione di accorgimenti *ad hoc* per la loro eliminazione o quanto meno riduzione ad un livello minimo (come previsto dalla legge).
- attività didattica : si sono svolti interventi formativi (alcuni di tipo "assembleare", altri più "mirati" in quanto rivolti agli Incaricati dei singoli reparti). I corsi assembleari sono stati predisposti secondo la procedura "e.c.m." e hanno contemplato una parte teorico-espositiva e una parte pratica idonea a coinvolgere il personale presente.

Le attività sopra indicate sono state descritte e formalmente riportate nel documento Report trasmesso periodicamente al Titolare e ai Responsabili del trattamento al fine di offrire agli stessi un quadro aggiornato e dettagliato della situazione in essere e i suggerimenti operativi su come procedere.

### **Misure da adottare**

In ottemperanza a quanto previsto dal Provvedimento del Garante Privacy pubblicato in G.U. n. 287 del 9 dicembre 2008, "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali", l'Azienda ospedaliera adotterà le seguenti misure finalizzate a garantire che la rottamazione del pc e conseguente cancellazione dei dati avvenga nel rispetto della Privacy:

### **Misure tecniche preventive**

Protezione dei file mediante password di cifratura, oppure memorizzazione dei dati su hard disk o su altri supporti magnetici usando sistemi di cifratura automatica al momento della scrittura.

### **Misure tecniche di cancellazione sicura**

La cancellazione sicura delle informazioni su disco fisso o su altri supporti magnetici è ottenibile con programmi informatici di "riscrittura" che provvedono - una volta che l'utente abbia eliminato dei file dall'unità disco con i normali strumenti previsti dai sistemi operativi (ad es., con l'uso del "cestino" o con comandi di cancellazione) - a scrivere ripetutamente nelle aree vuote del disco. Si possono anche utilizzare sistemi di formattazione a basso livello degli hard disk o di "demagnetizzazione", in grado di garantire la cancellazione rapida delle informazioni.

### **Smaltimento di rifiuti elettrici ed elettronici**

Per la distruzione degli hard disk e di supporti magnetici non riscrivibili, come cd rom e dvd, è consigliabile l'utilizzo di sistemi di punzonatura o deformazione meccanica o di demagnetizzazione ad alta intensità o di vera e propria distruzione fisica

## **8. CRITERI E MODALITA'PER IL RIPRISTINO DATI (regola 19.5 Disciplinare tecnico)**

Al fine di garantire il ripristino dei dati entro i termini di legge, è stata definita una procedura per l'esecuzione del backup che consente il salvataggio dei dati attraverso l'utilizzo di un sistema di backup centralizzato.

### **PROCEDURA DI GESTIONE BACKUP**

#### **1. OGGETTO E SCOPO**

La procedura definisce le modalità con cui sono gestite le attività di Backup dei dati memorizzati nei Server localizzati presso la Sala Macchine del SIA.

#### **2. CAMPO DI APPLICAZIONE**

Le attività di Backup che vengono eseguite giornalmente riguardano i database relativi ai seguenti applicativi software:

Gestione CUP, ADT, Pronto soccorso (Aurora Web)
Laboratorio Analisi (Powerlab)
Radiologia (RA2000)
Piattaforma regionale d'integrazione CRS-SISS
Gestione Personale (WHR)
Gestione economico-finanziaria (ENCO)
Gestione database Reparto Oncologia
PSICHE2000
PACS

### 3. MODALITÀ OPERATIVE

#### Tempistica

Le operazioni di backup sono a cadenza giornaliera in orari notturni e sono suddivise in due macroattività l'export dei dati e l'export delle configurazioni dei server.

#### Tipologia di export

L'export è sia di tipo "Full Database" che di tipo incrementale. Con cadenza giornaliera viene esportato l'intero database che comprende la struttura e i dati delle tabelle di produzione, struttura e dati delle tabelle di sistema. Per i database Oracle è previsto anche un export di RMAN, che consente un full export particolarmente sicuro e permette di tornare ad una situazione consistente in un determinato istante temporale. Questo consentirà di ricreare l'intero database su un altro server in caso di crash.

#### Export dei dati

L'export dei dati è effettuato automaticamente sui server dove risiedono i database.

#### Backup

Il backup di un export è effettuato automaticamente dal server dove vengono creati i file di export dei dati. Il backup inizia al termine dell'attività di export. Gli altri tipi di backup avvengono in un singolo passaggio e sono effettuati dagli agent di backup distribuiti, direttamente verso un sistema Storage Area Network.

Il backup del database del sistema di contabilità (Enco-GPI) non è effettuato tramite sistema centrale ma sui dischi di sistema locali.

Il salvataggio viene eseguito dal lunedì al sabato in una directory del DB Serve ( linux) e in una directory dell'Application Server (Windows 2003).

E' inoltre schedulata una copia giornaliera su cassetta di backup.

Il salvataggio del Database Psiche viene eseguito tramite Export giornaliero di Oracle.

E' in corso un'attività di assessment finalizzata all'estensione dell'utilizzo del sistema di backup centralizzato (Time Navigator) a tutti i database aziendali.

Il salvataggio dell'archivio delle immagini del sistema PACS è effettuato tramite sistema dedicato (Tivoli Storage Manager)

## **9. PIANIFICAZIONE INTERVENTI FORMATIVI (regola 19.6 Disciplinare tecnico)**

Si sono svolti interventi formativi degli Incaricati del trattamento, 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.

Pertanto, in applicazione di tale regola, nel corso del 2010 si sono svolti incontri di formazione in materia di Privacy in occasione dei quali sono stati esaminati i seguenti punti rilevanti della disciplina:

- introduzione
- definizioni principali (dato personale, dato sensibile, trattamento, ecc.)
- informativa (modalità ordinaria semplificata)
- consenso (modalità ordinaria e semplificata)
- soggetti attivi del trattamento (Titolare, Responsabili e Incaricati)
- misure di sicurezza (per il trattamento del dato cartaceo e informatico)
- misure di garanzia (analisi dell'art. 83 e correlato provvedimento dell'Autorità Garante)
- disposizioni particolari
- sanzioni (penali, civile, amministrative)
- casistica giurisprudenziale e comunicati dell'Autorità Garante

In aggiunta ai predetti incontri di tipo assembleare si sono altresì esaminati, in occasione della attività di *audit* svolta in collaborazione con la società di consulenza e riportati nelle apposite relazioni periodicamente trasmesse, i rischi che incombono sui dati, le misure disponibili per prevenire eventi dannosi, i profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, le responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

- Il calendario prevede incontri in loco – presso le strutture sanitarie e amministrative che svolgono operazioni di trattamento dati – da attuarsi tramite la società di consulenza

In aggiunta a ciò saranno concordati incontri di tipo assembleare con la collaborazione del competente Ufficio Formazione.

## **10. TRATTAMENTI AFFIDATI ALL'ESTERNO (regola 19.7 Disciplinare tecnico)**

L'Azienda ha affidato il trattamento dei dati in tutto o in parte a soggetti terzi in modalità *outsourcing* e ha nominato formalmente, per iscritto, tali soggetti quali Responsabili (esterni) del trattamento che si affiancano ai Responsabili interni (Dirigenti sanitari e amministrativi).

Tali Responsabili del trattamento devono rispettare gli obblighi ed gli oneri previsti dal Codice circa il trattamento dei dati nonché la legittimazione passiva nell'ipotesi di violazione delle predette disposizioni. In particolare il Responsabile del trattamento deve

- garantire il pieno rispetto delle disposizioni in materia di trattamento, compreso il profilo relativo alla sicurezza, e le connesse procedure aziendali da parte degli Incaricati;
- attenersi alle istruzioni impartite dall'Azienda ospedaliera che, anche tramite verifiche ispettive periodiche, vigila sulla puntuale osservanza delle proprie istruzioni;
- non effettuare in alcun modo trattamenti autonomi di dati raccolti e trattati in qualità di Responsabile;
- provvedere alla nomina dei propri collaboratori quali Incaricati del trattamento dati e definire l'ambito di trattamento dati al quale gli stessi possono avere accesso;
- consentire all'Azienda ospedaliera di effettuare i controlli e la vigilanza sulla corretta osservanza delle disposizioni di legge e delle istruzioni presenti e future impartite;
- valutare e adottare le misure di sicurezza idonee e preventive, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati medesimi, provvedendo, con cadenza almeno semestrale, ad inoltrare all'Azienda la comunicazione in ordine alle misure di sicurezza adottate;

- segnalare con tempestività al Titolare eventuali problemi relativi all'applicazione della disciplina di cui al D.Lvo. 196/2003 riscontrati nell'esercizio delle attività di competenza.

### Attestazione di conformità

L'Azienda ospedaliera, nel perseguire le proprie finalità di trattamento, può avvalersi di un soggetto esterno alla propria struttura per la fornitura e installazione di *software* e *hardware* nonché per l'erogazione di servizi aventi ad oggetto le misure minime di sicurezza come indicate dal decreto legislativo n. 196/2003.

Rispetto a tali soggetti esterni l'Azienda, conformemente a quanto previsto dal punto 25 del Disciplinare tecnico, si riserva la facoltà di ricevere dal fornitore/installatore/soggetto esterno una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del medesimo disciplinare tecnico a mezzo seguente *template*:

#### **TEMPLATE PER DICHIARAZIONE DI CONFORMITA'**

NOME SOCIETA'	<i>Indicare il nome del soggetto terzo installatore e/o erogatore del servizio</i>
ATTIVITA' SVOLTA	<i>Descrivere l'attività svolta, in particolare se trattasi di installazione SW/HW o servizi</i>
CONTRATTO N.	<i>Indicare il riferimento contrattuale</i>
DICHIARAZIONE	<i>Descrivere l'attività svolta nell'interesse dell'Azienda ospedaliera e attestare la conformità della stessa a quanto stabilito dal Disciplinare tecnico in materia di misure minime di sicurezza.</i>
DATA E FIRMA	<i>Firma del legale rappresentante</i>

## **11. SEPARAZIONE DEI DATI IDENTIFICATIVI (regola 19.8 Disciplinare tecnico)**

Attualmente la maggior parte dei software utilizzati dall'Azienda non consente la separazione dei dati personali (anagrafiche) dai dati inerenti lo stato di salute.

E' stata effettuata, di concerto con i fornitori dei singoli applicativi, la riconfigurazione degli stessi applicativi al fine di consentire la cifratura delle transazioni e di adempiere a tale misura.

Con l'integrazione di questa Azienda Ospedaliera al progetto CRS-SISS, la Regione Lombardia per il tramite di Lombardia Informatica ha fornito sia nuovi server che le necessarie licenze del Database Oracle con cui è stato possibile implementare la crittografia delle transazioni.

Tale database, oltre ad essere riconosciuto come uno dei database più sicuri a livello mondiale, consente di implementare una modalità di crittografia a 128 bit per cui tutti gli scambi di dati tra server ed i vari clients non avvengono "in chiaro", in altre parole le informazioni (anagrafiche, cliniche, amministrative) prima di essere spedite dal server al client tramite protocollo di rete (TCP-IP), sono crittografate ed a loro volta vengono decrittografate in tempo reale quando raggiungono il client; questo rende praticamente impossibile l'intercettazione di alcun dato sulla rete.

Questa modalità è attualmente attiva per i seguenti ambiti:

- tutti i Laboratori (Laboratorio analisi, trasfusionale, medicina nucleare);
- tutti i reparti;
- tutte le casse (CUP);
- Anatomia patologica;
- Pronto Soccorso.

## 12. PROGETTO CRS - SISS

### Impatti di sicurezza

#### Impatti architetturali

La interconnessione del sistema informatico della A.O con il CRS-SISS avviene tramite il PdL (Posto di Lavoro) o tramite il F.E (Front End della porta Applicativa). Mentre il F.E. è sempre configurato e gestito dal progetto senza intervento né di tipo applicativo né sistemistico da parte della azienda, il PdL sia in configurazione per supportare gli accessi di tipo Application to Application, che nella configurazione in cui interagisce con il CRS-SISS via Web Browser, dopo una iniziale installazione e configurazione fatta dal progetto è gestito direttamente dalla azienda Ospedaliera. La gestione dei PdL SISS rientra nella normale gestione di tutti i PdL dell'Azienda Ospedaliera, valgono pertanto le disposizioni illustrate nel DPS della stessa A.O. Tali disposizioni possono essere brevemente riassunte come segue:

- Installazione di un sistema antivirus su ogni PdL gestito centralmente;
- Accesso ai PdL tramite credenziali gestite centralmente;
- Autenticazione di tipo "forte" sin dall'accesso al singolo PdL tramite sistema di Single Sign On basato su Smart Card SISS in fase di attuazione sui PdL in ambito sanitario e di prossima estensione sui PdL in ambito amministrativo;
- Adozione di un sistema di "Patch Management" per l'aggiornamento automatico dei singoli PdL con i vari aggiornamenti rilasciati dai singoli fornitori sia del software di base (Sistema Operativo) che applicativo.

#### Impatti operativi

Gli scambi fra l'A.O e la Regione Lombardia, con lo scopo di fornire alla Regione i dati relativi alle prestazioni erogate agli assistiti ai fini della contribuzione, avviene adottando le seguenti misure di sicurezza:

- la base dati centralizzata della Regione Lombardia (Dominio Centrale) è concepita per separare logicamente e anche fisicamente i dati anagrafici da quelli afferenti gli eventi

sanitari di rilevanza amministrativa. In questo modo non è possibile ricavare informazioni sullo stato di salute di un assistito avendo accesso ad un solo insieme omogeneo di dati;

- gli operatori hanno accesso ai servizi applicativi solo a seguito di un processo di autenticazione e autorizzazione realizzato mediante sistema basato su un'infrastruttura a chiavi pubbliche (PKI) ed utilizzo di smart card operatore;
- la trasmissione di documenti e di flussi di dati, firmati elettronicamente ove previsto, è criptata con chiave privata in modo da renderne inutile l'intercettazione.

Gli operatori del servizio sanitario (es. medici e dirigenti sanitari di strutture socio-sanitarie, medici di medicina generale, pediatri di libera scelta), sono ammessi ad accedere ai dati di un paziente custoditi da altre organizzazioni aderenti al progetto SISS a seguito di espressa autorizzazione del paziente medesimo, adottando le seguenti misure di sicurezza:

- l'operatore sanitario che effettua la transazione ha accesso al servizio applicativo solo a seguito di un processo di autenticazione e autorizzazione basata sulla carta operatore;
- i dati relativi ad ogni singolo paziente sono disaggregati all'origine. Essi rimangono registrati nei vari archivi coinvolti (quelli delle singole organizzazioni che hanno erogato prestazioni a quel paziente) e vengono aggregati solamente quando ciò è necessario, su espressa autorizzazione dell'interessato;
- l'autorizzazione espressa dal paziente all'aggregazione estemporanea dei dati che lo riguardano è attuata mediante consegna all'operatore da parte del paziente della propria Carta dei Servizi, che lo identifica univocamente. Senza questa autorizzazione la transazione informatica non può essere eseguita;
- nei casi di situazioni di emergenza sanitaria (espressamente previsti nell'ambito del SISS) i medici possono accedere ai dati sanitari anche in assenza della Carta dei Servizi dell'assistito;
- il medico ospedaliero può accedere liberamente ai dati degli assistiti ricoverati presso il proprio reparto.

## **Impatti organizzativi**

L'azienda Ospedaliera in qualità di Responsabile del Trattamento dei dati attinenti al progetto Siss, ha provveduto a nominare formalmente il proprio personale, Incaricato del trattamento che eroga ed accede ai servizi del Siss.

Ogni operatore è ammesso esclusivamente all'accesso di un numero specifico di funzioni in base al proprio ruolo e alle proprie responsabilità. Il criterio di autorizzazione si applica a livello di programma, di funzione applicativa e di singolo elemento di dati di una transazione.

Il personale incaricato è stato adeguatamente formato prima di iniziare ad operare sul progetto e sono inoltre previsti momenti formativi di richiamo per mantenere elevata la attenzione alle problematiche di sicurezza.

I contenuti della formazione di sicurezza effettuata sono stati i seguenti: le responsabilità personali, la gestione sicura degli elementi individuali di Identificazione ed Autenticazione, il comportamento da tenere in presenza di violazioni delle procedure di sicurezza.

## **Infrastruttura di sicurezza**

### Trattamenti interessati

L'Azienda ospedaliera svolge le operazioni di trattamento come identificate nel Progetto SISS e di seguito indicate:

- l'Azienda ospedaliera relativamente a trattamenti per finalità amministrative, è Titolare dei trattamenti di registrazione, organizzazione, conservazione, consultazione, elaborazione, selezione, estrazione, interconnessione, raffronto, utilizzo e comunicazione relativi a prescrizioni, prenotazioni, erogazioni, eventi sanitari, esenzioni, flussi di rendicontazione e anagrafica;
- l'Azienda ospedaliera relativamente a trattamenti per finalità di cura, è Titolare dei trattamenti di registrazione, conservazione, elaborazione, selezione, estrazione, interconnessione, raffronto e comunicazione relativi alla gestione delle basi dati inerenti all'utilizzo del Fascicolo Sanitario Elettronico (FSE) e del consenso.

## 2.2 Responsabilità e organizzazione di sicurezza

<b>RUOLO</b>	<b>RESPONSABILITA'</b>
Responsabile dei Servizi <b>Direttore Generale</b>	<i>Coordina le attività della propria organizzazione e la impegna formalmente verso il CRS-SISS. E' il responsabile gerarchico della azienda che aderisce al progetto.</i>
Manager della sicurezza	<i>Responsabile del management della sicurezza per la propria organizzazione, elabora, aggiorna e pubblica la politica di sicurezza dei sistemi informativi, con particolare riguardo alle misure da adottare per la sicurezza dei servizi nell'ambito del CRS-SISS. Coordina la redazione DPS e delle Istruzioni Operative. Sovrintende alla corretta e puntuale applicazione della Policy definita.</i>
Data Protection Manager	<i>Definisce appropriate misure per la conservazione ed il trattamento dei dati personali nella la propria organizzazione e verifica l'applicazione di tali misure per il corretto adempimento delle norme sul trattamento dei dati personali.</i>
Amministratore dei Sistemi e dell'Infrastruttura di Rete	<i>È responsabile dell'amministrazione del software, hardware e infrastruttura di rete. Effettua monitoraggio ed auditing delle misure tecniche di sicurezza.</i>
Referente IRT	<i>È il riferimento per l'IRT(Incident Response Team) del CRS-SISS e per tutte le comunicazioni con il personale inerenti la continuità o la sicurezza del servizio.</i>
Operatore / Addetto <b>Personale sanitario ed amministrativo che eroga i servizi del Siss</b>	<i>Personale <b>INCARICATO</b> del trattamento che eroga ed accede ai servizi del CRS-SISS</i>

### Formazione Incaricati interni

Al piano di formazione che l'Azienda ospedaliera già adotta per tutti gli incaricati nominati deve essere aggiunta la parte riguardante il Progetto CRS-SISS e deve trattare i seguenti argomenti:

- gestione sicura della smart card operatore con specifico riferimento alle tipologie di carte operatore previste (Carta Nominativa, Carta Intestata, Carta Non Intestata);
- ripartizioni dei compiti in funzione del ruolo svolto dall'operatore.

Nel piano devono essere previsti momenti formativi di richiamo per mantenere elevata la attenzione alle problematiche di sicurezza.

Il dettaglio del piano di formazione, così come il processo di gestione e contabilizzazione della formazione, può far parte di una specifica Istruzione Operativa che va opportunamente referenziata.

### Gestione del rischio

Inoltre riportiamo di seguito le procedure e le misure specifiche della interconnessione con il CRS-SISS, nonché la procedura di Gestione delle Carte a Microprocessore.

Ogni potenziale utente dei sistemi o delle banche dati è associato ad un identificativo (user-id). Prima che un Utente acceda al sistema, agli archivi informatici o alla rete, ne **“deve”** essere verificata l'identità mediante un successivo livello di controllo **“autenticazione”**.

La verifica della identità dell'utente avviene secondo due procedure:

- la procedura, basata sulla Carta a Microprocessore e definita come **“Strong Authentication”**, viene impiegata per autenticare l'utente che accede ai servizi offerti dal SISS;
- la procedura basata sulla conoscenza da parte dell'utente di un segreto (password), viene impiegata per autenticare l'utente quando accede a quegli altri servizi disponibili sul sistema locale.

Dopo il riconoscimento autenticato dell'utente e prima di consentire allo stesso l'accesso ai dati, la validità della richiesta di accesso è verificata con un controllo basato su una politica di controllo accessi **“chiusa”**, cioè nel senso che **“tutto ciò che non è esplicitamente concesso è vietato”**. Lo schema di autorizzazione per l'accesso alle risorse / servizi in uso **“è”** valutato, con riguardo alle

necessità operative degli incaricati, ciascun incaricato “è” ammesso a trattare soltanto i dati che sono strettamente necessari alla sua funzione, tale schema “deve” essere riveduto regolarmente. Le applicazioni e le infrastrutture inerenti l’erogazione dei servizi SISS applicano un criterio di autorizzazione d’accesso basato su ruoli, che prevede un ambito di diffusione dei dati strettamente necessario alle esigenze degli incaricati. Non “è” mai permesso l’accesso alle risorse (dati, servizi, sistemi) se non dopo una corretta identificazione ed autenticazione dell’incaricato.

### **Gestione Carte a Microprocessore**

L’Azienda Ospedaliera, tramite il proprio Responsabile Adesioni e Carte, si attiene a quanto prescritto dal CRS-SISS per la presa in carico delle Carte a Microprocessore e per la loro distribuzione ai Titolari (Operatori sociosanitari). destinatari delle Carte.

Il Manager della Sicurezza dell’azienda sociosanitaria predispone un piano di formazione a cui sottoporre ciascun Titolare della Carta prima del rilascio della Carta stessa.

Con cadenza Annuale, Il Manager della Sicurezza effettua a tutti i Titolari delle Carte un incontro di richiamo incentrato sui punti:

- Responsabilità dell’utilizzo e della custodia delle Carte a Microprocessore.
- Cura nella gestione confidenziale del Personal Identification Number (PIN) di accesso alla Carta.
- Maggiori difficoltà incontrate nella gestione delle Carte.
- La Carta a Microprocessore riveste per l’Operatore della azienda sociosanitaria una doppia funzione:
  - Permette all’Operatore di essere Identificato ed autenticato dal CRS-SISS in modalità Forte.
  - Permette all’Operatore di firmare digitalmente i documenti informatici scambiati con il CRS-SISS.
- La validità e la sicurezza di ciascuna delle due funzioni si basa, oltre che naturalmente sulla robustezza intrinseca degli algoritmi crittografici e sulla affidabilità e correttezza della Struttura (PKI) che rilascia e gestisce i certificati (Certification Authority), su due fondamentali requisiti a carico dell’Operatore della azienda sociosanitaria:
  - Il possesso della carta da parte dell’Operatore Titolare della Carta.

- La conoscenza esclusiva da parte dell'Operatore Titolare della Carta del Codice segreto (PIN) che abilita la funzione prescelta (Autenticazione / Firma-Digitale).

### **Inizializzazione**

- Il Titolare della carta deve, dopo la procedura di generazione dei parametri per la Autenticazione Forte (chiavi e certificato), modificare il PIN di default che successivamente lo abiliterà a questa funzione.
- Il Titolare della carta deve, subito dopo aver eseguito la inizializzazione della Carta, modificare il PIN di default di abilitazione alla funzione di Firma Digitale.
- I PIN devono avere una lunghezza di 8 caratteri. Nella scelta degli 8 (otto) si seguono le regole in vigore per la generazione della password .
- Si raccomanda che i due PIN non siano creati identici.

### **Utilizzo e Gestione**

- I PIN di accesso alle funzioni (autenticazione e firma), relative ad un Operatore Titolare di carta sono strettamente personali e non devono assolutamente essere comunicati ad altri.
- L'Operatore Titolare di carta deve evitare di trascrivere i PIN in chiaro, su carta o su altro supporto informatico.
- L'Operatore Titolare di carta è espressamente invitato a modificare il PIN nei casi in cui ritenga compromessa la confidenzialità.
- L'Operatore Titolare di carta deve archiviare in modo sicuro i due codici PUK (PIN Unblocking Key), con i quali gli è possibile sbloccare la Carta a Microprocessore dopo il ripetuto (7 volte) inserimento errato del PIN.
- La perdita della Carta a Microprocessore o la compromissione dei codici PUK, deve essere prontamente comunicata dall'Operatore Titolare alla Certification Authority (CA), secondo la procedura definita nel Manuale Operativo della CA per la richiesta di revoca dei certificati.
- L'Operatore Titolare di carta deve gestire con diligenza la Carta a Microprocessore assegnatagli, evitando le situazioni in cui ne perda il controllo (es. lasciare la Carta incustodita). L' Operatore Titolare di carta deve prontamente segnalare al proprio Manager

della Sicurezza le violazioni di sicurezza relative alle Carte a Microprocessore. Tra le violazioni di sicurezza sono incluse quelle situazioni in cui all'Operatore Titolare di carta viene richiesto, specialmente se da parte di altri utenti del CRS-SISS, di comunicare i propri PIN di abilitazione.

### **Carta Non Intestata**

Le regole di gestione sopra riportate, sono valide per tutte le tipologie di carte operatore (Carta Nominativa, Carta Intestata, Carta Non Intestata).

Per la specifica tipologia della Carte Non Intestate si riportano ulteriori considerazioni di sicurezza come dedotte dal documento (rif [3]).

### **Caratteristiche della Carta Non Intestata**

La carta 'non ad personam' (ovvero non intestata) è stata pensata per gli operatori CRS-SISS per i quali non è prevista la possibilità di firma digitale. La soluzione prevede smartcard con le seguenti caratteristiche:

- sul fronte della smartcard non è indicato nominativo della persona;
- non avere diritto di firma.

Le informazioni di carattere organizzativo che verranno stampate sulle carte non intestate sono:

- Nome Struttura: Azienda e Presidio;
- Nome del Servizio/Reparto a cui appartiene l'operatore al quale tale carta è/verrà assegnata;
- Data di emissione della carta.

I ruoli applicativi che potranno prevedere l'uso di queste smartcard sono:

- Farmacista Collaboratore;
- Amministrativo di Azienda;
- Impiegato ASL di Scelta/Revoca;

- Ufficio Privacy;
- Infermiere;
- Altro Operatore di Emergenza;
- Operatore di Call-center;
- Impiegato del Punto di Adesione/ Punto di Registrazione ( PdA/PdR).

L'utilizzo di tale tipologia di carta, per i ruoli sopra descritti, è consigliata in quei contesti organizzativi che si caratterizzano per un elevato turnover o rotazione del personale a parità di ruolo e mansione (es. nel caso in cui vi sono frequentemente collaborazioni esterne o contratti a termine).

In questi casi, la struttura può preventivamente richiedere carte non intestate pur non conoscendo i nominativi delle persone alle quali dovranno essere assegnate.

Queste carte verranno poi attivate nel momento in cui sarà noto l'operatore al quale assegnarle, minimizzando così i tempi necessari per rendere operativo nel CRS-SISS il nuovo operatore grazie all'anticipazione del processo di produzione.

Le carte non intestate che vengono richieste verranno consegnate al PdA/PdR di riferimento del richiedente (e.g. PdA/PdR della ASL per i MMG, PdA/PdR dell'Azienda per le AO).

Nel momento in cui un operatore dovrà essere dotato di una carta non intestata, dovrà recarsi presso il PdA/PdR.

Nel caso in cui la carta richiesta sia disponibile, il PdA/PdR genererà la quantità di sicurezza e attiverà la carta che potrà essere consegnata all'operatore; in caso contrario il PdA/PdR richiederà la produzione della carta richiesta e successivamente genererà la quantità di sicurezza e attiverà la carta che potrà essere consegnata all'operatore.

Solo nel momento in cui una carta non "ad personam" (ovvero non intestata) viene assegnata ad un operatore viene generata la relativa quantità di sicurezza (i.e. codici PIN/PUK, ecc.).

Quando l'operatore non dovrà più utilizzare il CRS-SISS presso la struttura che l'aveva dotato di carta non intestata, dovrà restituire la carta alla PdA/PdR di riferimento.

I programmi realizzati dal progetto CRS-SISS:

- sono installati e configurati da LISIT (porta applicativa) e da accreditati Provider di servizi (posto di lavoro);

- vengono periodicamente monitorati dal Centro Gestione Integrata (CGI) del progetto;
- garantiscono che:
  - i dati sanitari “sono” trasmessi in rete protetti da adeguati algoritmi di cifra;
  - i dati sanitari quando presenti negli archivi informatici “sono” memorizzati cifrati o disaggregati dai dati personali in modo che la loro compromissione non permetta di ricondurre il dato sanitario alla specifica persona.

#### Sicurezza della connettività al Crs – Siss

L'amministratore dei sistemi della azienda ospedaliera, in caso di prima installazione, configurazione o manutenzione degli apparati di interconnessione con il CRS-SISS opera come segue:

- Prima di permettere l'accesso agli apparati, verifica l'identità del personale inviato dal Provider. A tal riguardo il Provider è tenuto ad informare preventivamente l'azienda sulla propria procedura di installazione/manutenzione evidenziando i momenti di controllo che l'azienda può esercitare.
- Durante l'attività svolta dal personale del Provider, esercita una supervisione diretta sulle attività condotte dal personale del Provider.
- Nel caso il personale del Provider debba accedere al sistema informativo senza restrizioni di accesso, si cautela preventivamente mediante rimozione o cifratura dei dati di privacy.
- Al termine dell'installazione, l'amministratore dei sistemi della azienda prende in carico gli apparati secondo le regole di gestione degli stessi, mediante la sottoscrizione del verbale di collaudo che il personale del Provider rilascia firmato per attestare l'esito positivo dei controlli e delle attività di installazione e/o manutenzione eseguita.

#### **Contributi dei Responsabili designati**

L'Azienda ha scaricato tramite il SIA, dall'area riservata del sito di Progetto ([www.crs.lombardia.it](http://www.crs.lombardia.it)) i "contributi", aggiornati per il Documento Programmatico sulla Sicurezza 2011 (DPS), delle Aziende Informatiche designate Responsabili dei trattamenti nell'ambito del Progetto CRS-SISS.

Le Aziende Informatiche designate RESPONSABILI “contribuiscono” al presente DPS fornendo un riferimento costituito da:

- nome del documento nel quale la singola Azienda RESPONSABILE ha descritto come sono stati realizzati gli interventi operativi necessari per rispondere ai requisiti di sicurezza indicati nell'atto di designazione;
- indicazione della collocazione (nel sistema documentale dell'Azienda) di tale documento.

I contributi", che si riportano di seguito sono relativi a:

Lombardia Informatica S.p.A.

Lutech S.p.A.

Almaviva S.p.A.

Santer Reply S.p.A.

Transcom Worldwide S.p.A.

#### Contributo DPS da parte di Lombardia Informatica SpA

Il contributo di **Lombardia Informatica SpA** in quanto **RESPONSABILE** di trattamento di dati nell'ambito del Progetto CRS-SISS, ai sensi della DGR N. VIII 5198 del 02/08/2007, è contenuto nel documento: LI-SG-DPS#11 "DOCUMENTO PROGRAMMATICO SULLA SICUREZZA -Edizione 2011 (ai sensi del D.Lgs. 196 /2003)", Capitolo "Adempimenti di sicurezza per i trattamenti relativi al Progetto CRS-SISS di cui Lombardia Informatica è RESPONSABILE".

Il documento è pubblicato nella *intranet* aziendale.

#### Contributo DPS da parte di Almaviva SpA

Il contributo di **Almaviva S.p.A** in quanto **RESPONSABILE** di trattamento di dati nell'ambito del Progetto CRS-SISS ai sensi della DGR N. VIII 5198 del 02/08/2007, è contenuto nei documenti :

- CRSSISS-FORM-MIN-01[rel.4] Progetto CRS-SISS - Adempimenti di sicurezza per i trattamenti relativi al servizio "Formazione e Addestramento";
- CRSSISS-PRIV-MIN-01 [rel.4] Progetto CRS-SISS - Adempimenti di sicurezza per i trattamenti relativi al servizio "Gestione Privacy";

I documenti sono archiviati presso la sede di Almaviva SpA, Via dei Missagli, 97 B/4 - 20142 Milano.

#### Contributo DPS da parte di Lutech SpA

Il contributo di **Lutech S.p.A** in quanto **RESPONSABILE** di trattamento di dati nell'ambito del Progetto CRS-SISS, ai sensi della DGR N. VIII 5198 del 02/08/2007, è contenuto nel documento: DPS ver. 05 del 14.02.2011.

Il documento è tenuto presso l'Ufficio Legale di Lutech SpA, in Via Mozart, n. 47 - 20093 Cologno Monzese (MI).

#### Contributo DPS da parte di Santer Reply SpA con Unico Azionista

Il contributo di **Santer Reply S.p.A** in quanto **RESPONSABILE** di trattamento di dati nell'ambito del Progetto CRS-SISS, è contenuto nel documento: Documento Programmatico sulla Sicurezza (DPS) - Santer S.p.A. con Unico Azionista.

All'interno dell'impianto documentale di Santer la sua collocazione è nella cartella "*Santer Corporate Documentation*", all'interno del *folder* "Privacy" sulla *intranet* aziendale (KM42).

#### Contributo DPS da parte di Transcom Worldwide S.p.A.

Il contributo di **Transcom Worldwide S.p.A.** in quanto **RESPONSABILE** di trattamento di dati nell'ambito del Progetto CRS-SISS, è contenuto nel documento:

Documento Programmatico Sulla Sicurezza Dei Dati - Codice In Materia Di Dati Personali & Disciplinare Tecnico In Materia Di Misure Minime Di Sicurezza (Decreto Legislativo 30 Giugno 2003 n. 196) - Rev. 5 2011: Cap. 4 "Elenco dei trattamenti di dati personali" e Cap. 7 "Misure di sicurezza adottate".

Il documento è archiviato presso la sede legale di TRANSCOM WORLDWIDE SpA, via Brescia, 28 – 20063 Cernusco sul Naviglio Milano

### **13. AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO**

Conformemente a quanto previsto dal punto 26 del Disciplinare tecnico, l'Azienda ospedaliera in qualità di Titolare del trattamento riferisce nella relazione accompagnatoria del bilancio d'esercizio dell'avvenuto aggiornamento del documento programmatico sulla sicurezza entro il termine di legge.

A tale documento si allegano quale parte integrante dello stesso:

- Il regolamento relativo ai sistemi di videosorveglianza utilizzati ai fini di sicurezza dal titolo "REGOLAMENTO PER LA GESTIONE DEI SISTEMI DI VIDEOSORVEGLIANZA DELL'A.O. FATEBENEFRAPELLI E OFTALMICO" (allegato 1)
- L'analisi dei rischi relativa alla sicurezza informatica (allegato 2)

Milano, 31 marzo 2011

Il Direttore Generale

Dr. Giovanni Michiara