DETERMINAZIONE N. 791 del 02 APR. 2014 Atti n. 617/2013 all.2

AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA – ANNO 2014

IL DIRETTORE GENERALE

VISTO il decreto legislativo n. 196 del 2003 Codice in Materia di Protezione Dei Dati Personali;

VISTO anche il Regolamento per il trattamento dei dati sensibili e giudiziari di competenza della Giunta regionale, delle aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione Lombardia (artt. 20-21 del D.Lgs. n. 196/2003) del 24 dicembre 2012, pubblicato sul Bollettino Ufficiale (BURL) supplemento n.52 in data 27 dicembre 2012 .(Atti 167/2011 all.36);

RICHIAMATA integralmente la propria determinazione n. 914 del 31 marzo 2006 con la quale:
- è stato formalizzato, in atti n. 752/2000 all. 43, il Documento Programmatico sulla Sicurezza;
- è stata disposta la formale notifica al garante dei trattamenti di dati genetici e di dati idonei a rivelare lo stato di salute e la vita sessuale;
- è stata assunta formalmente la nuova modulistica con le conseguenti procedure;

RICHIAMATA integralmente la propria determinazione n. 733 del 25 marzo 2013 con la quale sono stati formalizzati gli aggiornamenti per l'anno 2013 .

RITENUTA la necessità di aggiornare entro il 31 marzo 2014 il Documento Programmatico sulla Sicurezza in riferimento all'evoluzione del Sistema Informatico Aziendale della Fondazione.

DETERMINAZIONE N. 791 del 02 APR. 2014 Atti n. 617/2013 all.2

SENTITI i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario;

DETERMINA

di formalizzare, nel testo in atti n. 617/2014 all. 2 il Documento Programmatico sulla Sicurezza come aggiornato al 31 marzo 2014.

IL DIRETTORE GENERALE
Dott. Luigi MACCHI

IL DIRETTORE SANITARIO
Dr.ssa Anna Pavan

IL DIRETTORE AMMINISTRATIVO
Dott. Osvaldo Basilico

REGISTRATA NELL'ELENCO DELLE DETERMINAZIONI
IN DATA 02 APR. 2014 N. 791

Servizio competente: U.O.C. Qualità, Rischio, Accreditamento, Appropriatezza e Privacy
Responsabile del procedimento: Silvana Castaldi

DETERMINAZIONE N. 791 DEL 02 APR. 2014

V1 del 25.03.2013

Contributi 2013

delle Aziende Informatiche designate Responsabili del trattamento dei dati personali effettuato nell'ambito del SISS

PREMESSA

Nonostante la soppressione formale dell'obbligo della redazione del documento programmatico sulla sicurezza (DPS), molti TITOLARI hanno deciso di mantenere la redazione di un documento che persegue i medesimi obiettivi e scopi.

Di seguito i "contributi" delle Aziende Informatiche designate ***RESPONSABILI*** del trattamento nell'ambito SISS ed in particolare:

- **Lombardia Informatica SpA**;
- **Lutech SpA**;
- **Almaviva SpA**;

- **Transcom Worldwide SpA***;
- **Santer Reply SpA con Unico Azionista****

* non tutti i **TITOLARI** si avvalgono di **Transcom Worldwide SpA**, invitiamo i soli **TITOLARI** che hanno effettuato la designazione a **RESPONSABILE** per il trattamento di Prenotazione delle prescrizioni ad arricchire il proprio documento con il relativo contributo;

** non tutti i **TITOLARI** si avvalgono di **Santer Reply SpA con Unico Azionista**, invitiamo i soli **TITOLARI** che hanno effettuato la designazione a **RESPONSABILE** per i trattamenti di manutenzione delle banche dati della piattaforma Regionale di Integrazione ad arricchire il proprio documento con il relativo contributo ;

DATA DOCUMENTO 25.03.2012
VERSIONE 02
EMESSO DA Area supporto normativo e privacy office – Lombardia Informatica

Contributo DPS da parte di Lombardia Informatica SpA

Il contributo di **Lombardia Informatica SpA** in quanto ***RESPONSABILE*** di trattamento di dati nell'ambito del SISS, ai sensi della DGR N. VIII 5198 del 02/08/2007 è contenuto nel documento:

> *LI-SG-DPS - Rev. 03 – Documento Programmatico sulla Sicurezza – Edizione 2013*
> *Capitolo "Adempimenti di sicurezza per i trattamenti relativi al CRS-SISS di cui Lombardia Informatica è RESPONSABILE".*
> *Il documento è tenuto presso la sede legale di LOMBARDIA INFORMATICA SpA, Via Don G. Minzoni, 24 - 20158 Milano.*

Contributo DPS da parte di Almaviva SpA

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

> *SISS-PRIV-MIN-01 [rel.1] Progetto SISS - Adempimenti di sicurezza per i trattamenti relativi al servizio "Gestione Privacy".*
> *Il documento è archiviato presso la sede di Almaviva SpA, Via dei Missaglia, 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 CRS-SISS, ai sensi della DGR N. VIII 5198 del 02/08/2007 è contenuto nel documento:

> *Il documento nel quale sono descritte le misure di sicurezza adottate da Lutech è il DPS ver. 07 del 2013, tenuto presso l'ufficio legale di Lutech Spa in Cologno Monzese, via Mozart n. 47*

Contributo DPS da parte di Santer Reply SpA con Unico Azionista

Il contributo di **Santer Reply S.p.A. con Unico Azionista** in quanto ***RESPONSABILE*** di trattamento di dati nell'ambito del 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 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. 7 2013: Cap. 3 "Elenco dei trattamenti di dati personali" e Cap. 6 "Misure di sicurezza adottate".*
>
> *Il documento è archiviato presso la sede legale di TRANSCOM WORLDWIDE S.p.A., via Brescia, 28 – 20063 Cernusco sul Naviglio Milano*

FONDAZIONE IRCCS CA' GRANDA
OSPEDALE MAGGIORE POLICLINICO

Atti 617/2014, all. 2

Documento Programmatico sulla Sicurezza

31 marzo 2014

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

INDICE

INDICE DELLE TABELLE

1 INTRODUZIONE

Il presente documento disciplina il trattamento dei dati personali effettuato all'interno di tutte le strutture della Fondazione IRCCS CA' Granda Ospedale Maggiore Policlinico, mediante l'utilizzo di sistemi elettronici e non, ai sensi del D.Lgs.n.196/2003.
Il Documento Programmatico sulla Sicurezza (D.P.S.) valuta in maniera critica sia le misure di sicurezza indicate dal D. Lgs. n.196/2003, con particolare riferimento all'Allegato B, sia il piano programmatico di miglioramento.
In particolare nel D.P.S. si evidenziano le parti dedicate all'analisi dei rischi connessi ai trattamenti effettuati, all'analisi delle misure di controllo, al programma di formazione per gli incaricati, ai provvedimenti adottati e agli aggiornamenti da attuare.
Il documento contiene altresì tutte le indicazioni per definire il trattamento dei dati personali, i compiti e le responsabilità coinvolte.
Strumento utile per programmare e attuare l'adeguamento ai sensi di legge, il documento è finalizzato a garantire il rispetto della sicurezza dei dati trattati.
Nel D.P.S. vengono presi in esame i concetti di rischio e di sicurezza validi sia nei sistemi informatici che nei sistemi di comunicazione tradizionali.
La natura programmatica del documento si esprime nella necessità di un continuo aggiornamento del D.P.S. in quanto strumento utile a prevedere e prevenire le possibili situazioni di rischio.

L'elaborazione del presente "Documento Programmatico per la Sicurezza" si è basata su dati ottenuti a seguito di:

- analisi della situazione (verifica delle banche dati e dei trattamenti in atto);
- descrizione delle misure di sicurezza adottate per la protezione dei dati;
- descrizione delle misure di sicurezza da adottare (programma di miglioramento).

2 DEFINIZIONI

autentificazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità credenziali di autentificazione: i dati ed i dispositivi in possesso di una persona da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica

banca dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità, dislocate in uno o più siti

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

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

comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di comunicazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la comunicazione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato

credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica

crittografia: sistema che consente di rendere maggiore la sicurezza di un file tramite codifica. Una volta crittografato, per poter essere letto, il file deve essere decodificato

dati biometrici:i dati relativi alle caratteristiche fisiche o comportamentali di una persona (es. impronte digitali, scansione del palmo della mano /del volto/DNA)

dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) ad o) e da r) ad u) del DPR 14/11/2002 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

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

dati sensibili: i 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, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale

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

dato personale: qualunque informazione relativa a persona fisica identificata o identificabile anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso, un numero di identificazione personale

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

garante: l'autorità di cui all'art. 153, istituita dalla legge 31 dicembre 1996, n.675

incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

interessato: la persona fisica cui si riferiscono i dati personali

misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

parola chiave: componente di una credenziale di autenticazione associata ad una persona e a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti

responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente. associazione od organismo preposti dal titolare al trattamento dei dati personali

rete pubblica di comunicazioni: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico

separazione dei dati elettronici: i dati sensibili sono archiviati in tabelle/file separati da quelli contenenti i dati identificativi. Dove la separazione è realizzata, anche nel caso di intrusione nella banca dati il riconoscimento di un soggetto non sarebbe possibile senza una conoscenza completa delle relazioni tra gli oggetti componenti la struttura logica del database

servizio di comunicazione elettronica: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva nei limiti previsti dall'art.2 lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002

sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente

strumenti elettronici: gli elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento

titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitariamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità di trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza

trattamento: qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, la 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

3 ELENCO DEI TRATTAMENTI DI DATI PERSONALI

(regola 19.1)

La Fondazione IRCCS CA' Granda Ospedale Maggiore Policlinico si attiene per le operazioni di trattamento dati a quanto stabilito dal Codice in Materia di Protezione dei Dati Personali, D.Lgs.n.196/2003, e dal "Regolamento per il trattamento dei dati sensibili e giudiziari di competenza della Giunta regionale, delle aziende sanitarie, degli enti e agenzie regionali, degli enti vigilati dalla Regione Lombardia" (artt. 20-21 del D.Lgs. n. 196/2003) del 24 dicembre 2012, pubblicato sul Bollettino Ufficiale (BURL) supplemento n.52 in data 27 dicembre 2012 .

Il Regolamento è consultabile sul sito della Regione Lombardia www.regione.lombardia.it ed è pubblicato nell'internet della Fondazione in Bacheca Privacy nella sezione "Normativa"

L'elenco dettagliato dei trattamenti effettuati da ciascuna Unità Operativa della Fondazione IRCCS CA' Granda Ospedale Maggiore Policlinico è documentato nel REGISTRO PRIVACY compilato in prima stesura da ciascuna Unità Operativa/Servizio e annualmente aggiornato.

Nel REGISTRO PRIVACY ogni Unità Operativa ha messo in evidenza i trattamenti effettuati e i rischi correlati al trattamento dei dati.

Stante la procedura di riferimento P.22.F pubblicata nell'intranet di Fondazione in Qualità sono a carico del Responsabile di UOC/UOSD/Servizi alcune responsabilità di rilievo:

- individuare e specificare, attraverso la corretta compilazione della Sez. 1 del Registro Privacy i trattamenti di dati personali effettuati presso l'UOC/UOSD/Servizi e fornire tutte le informazioni inerenti i trattamenti in atto presso l'UOC/UOSD/Servizi;

- procedere, attraverso la compilazione della Sez. 2 del Registro Privacy, alla valutazione dei rischi incombenti sui dati personali trattati presso l'UOC/UOSD/Servizio;

- trasmettere, in formato elettronico ed in formato cartaceo il Registro Privacy correttamente compilato in ogni sua parte e debitamente sottoscritto dal Responsabile e dal Referente Privacy di UOC/UOSD/Servizio, all'indirizzo di posta elettronica del Responsabile del trattamento dei dati personali e presso l'Ufficio del medesimo sito in via F. Sforza, 28 Milano annualmente entro la fine del mese di febbraio e per l'anno in corso entro la fine di marzo;

- conservare presso l'UOC/UOSD/Servizi il Registro Privacy sottoscritto dal Responsabile del trattamento, rendere disponibile il documento integrale in occasione di visite ispettive interne e/o esterne e mantenere aggiornato il registro in formato elettronico e cartaceo.

Spetta invece al Responsabile del trattamento dei dati personali:
- censire i trattamenti in atto presso la Fondazione ai fini dell'annuale aggiornamento del DPS voluto dal Titolare del trattamento nonostante attualmente la tenuta del documento non sia obbligatoria;

- effettuare l'analisi dei rischi incombenti sui dati con particolare riferimento alle misure di sicurezza da adottare, all'accesso non controllato ai dati conservati in forma cartacea, all' intrusione fisica ed informatica e alla indebita cognizione di dati da parte di terzi durante le attività di diagnosi e cura;
- rendere disponibile il Registro Privacy in occasione di visite ispettive interne e/o esterne.

I REGISTRI PRIVACY sono disponibili presso il Responsabile del Trattamento dei dati personali e presso le singole UOC/UOSD/Servizi .

3.1 Censimento dati (senza l'ausilio di strumenti elettronici)

3.1.1 Direzione Generale e Servizi di Staff

Tabella 1 – Trattamento dati di Direzione Generale e Servizi di Staff

Trattamento	Dati sensibili e/o giudiziari	Descrizione del trattamento
Gestione Beni Culturali	Sì	Conservazione Archivio Amministrativo. Tenuta registri accettazione amministrativa. Rilascio certificato di ricovero.
Controllo di Gestione	Sì	Flusso informativo sale operatorie. Flusso assegnazione del personale al CDC. Scheda budget delle UU.OO.
U.O. Qualità,rischio, Accreditamento, appropriatezza e privacy	Sì	Comunicazione dati personali all'Ufficio Formazione. Consultazione dati cartelle cliniche e referti ambulatoriali relativi agli Audit interni Tutela dei trattamenti dati della Fondazione.
URP	Sì	Registrazione delle segnalazioni dell'utenza. Aggiornamento della Carta Servizi. Stipulazione contratti con associazioni. di volontari.
Ufficio Comunicazione	Si	Organizzazione di eventi interni ed esterni. Newsletter aziendale e scientifica. Piano di comunicazione aziendale. Trattamento eccezionale di dati sensibili.
Unità Organizzativa Sperimentazione Farmaci e Supporto Spedalità	Sì	Gestione convenzioni per consulenze con Enti e/o strutture private (attive e passive). Contratti con Case Farmaceutiche.
Settore Libera Professione		

Unità organizzativa Sviluppo e Promozione		
Servizio Prevenzione e Protezione	Sì	Gestione elenchi nominali del personale. Gestione giudizio idoneità. Compilazione scheda di destinazione lavorativa.
Progetti Speciali e Processi Amministrativi	Sì	Accordo di Programma .Procedure di Gara. Convenzioni con Enti.
Ufficio Affari Generali e Legali delle Assicurazioni	Sì	Relazioni con Broker e Assicurazioni Gestione sinistri
Progetto Archivio Centrale Cartelle Cliniche	Sì	Gestione Cartelle Cliniche – Archiviazione documentazione recente e remota. Consultazione. Predisposizione duplicati.

3.1.2 Direzione Amministrativa

Tabella 2 – Trattamento dati di Direzione Amministrativa

Trattamento	Dati sensibili e/o giudiziari	Descrizione del trattamento
Risorse Umane	Sì	Anagrafica e gestione giuridica del personale. Gestione Fascicoli del personale archiviati in un deposito chiuso a chiave.
Amministrazione e Finanze	Sì	Analisi dati per inserimento valori in contabilità ricevute e fatture (compresa l.p.). Gestione stipendi borsisti e consulenti. Dati patrimonio.
Approvvigionamenti	Sì	Raccolta dati dei pazienti in trattamento dialitico. Raccolta dati per offerte, ordini e bolle (fornitori).
Funzioni Tecniche	Sì	Procedure per il subappalto. Procedure per acquisti e/o spese, interventi in economia.
Patrimonio	Sì	Gestione ordinaria e straordinaria patrimonio immobiliare. Contenzioso.
Ingegneria Clinica	Sì	Raccolta dati per offerte, ordine, bolle (fornitori). Procedure per acquisti e spese in Economia.

3.1.3 Direzione Sanitaria

Tabella 3 – Trattamento dati di Direzione Sanitaria

Trattamento	Dati sensibili e/o giudiziari	Descrizione del trattamento

Accettazione	Sì	Raccolta dati personali e sensibili dei pazienti
Compilazione Cartella Clinica	Sì	I dati sensibili del paziente e dei suoi ascendenti vengono riportati in cartella dal medico che adotta misure cautelative atte a prevenire l'indebita conoscenza dei dati da parte di terzi. L'aggiornamento dati continua durante la degenza e in occasione dei controlli successivi nel rispetto della privacy.
Trattamenti terapeutici	Sì	Prescrizione e aggiornamento terapia.
Organizzazione e gestione documentazione sanitaria	Sì	Raccolta, riordino e archiviazione delle Cartelle Cliniche secondo criteri uniformi. Predisposizione duplicati e consegna agli aventi diritto.
Refertazione	Sì	Gestione referti, trascrizione in cartella, archiviazione e/o consegna all'interessato.
Prestazioni Ambulatoriali	Sì	Raccolta dati personali e sensibili dei pazienti nel rispetto della privacy.
Gestione liste d'attesa	Sì	Raccolta e aggiornamento dati anagrafici.
Gestione infortuni	Sì	Raccolta dati, elaborazione e trasmissione all'INAIL
Gestione dati Farmacia	Sì	Terapie infusionali personalizzate. Trasmissione dati pazienti, nel rispetto della privacy, alle ditte ed alle due dialisi. File F: invio dati all'AIFA
Servizio Sociale	Sì	Comunicazione con soggetti pubblici: Aziende Ospedaliere - Strutture e uffici del Ministero di Grazia e Giustizia etc... Comunicazione a soggetti privati: MMG-PLS, Comunicazione a cooperative sociali, enti convenzionati o accreditati
Soccorso Violenza Sessuale – S.V.S.	Sì	Anamnesi – Esame obiettivo – relazione Invio relazione autorità inquirente e/o autorità giudiziaria e/o servizi sociali ASL/Comune/ Provincia

3.1.4 Ulteriori trattamenti

Tabella 4 – Trattamento ulteriori dati

Settore	Attività delegate	Descrizione	Dati	Soggetto delegato
Sanitario	Prestazioni diagnostico - terapeutiche	Esami o trattamenti particolari non disponibili all'interno della Fondazione con	Dati anagrafici paziente. Dati sanitari necessari per esecuzione esame dia-	Altre strutture Sanitarie convenzionate con la Fondazione o, in

		invio all'esterno di campioni biologici o del paziente stesso.	gnostico o tratta- mento richiesto.	emergenza, anche non convenzionate.
Servizi ausiliari in appalto/interinali	Assistenziali e di supporto. Riabilitazione	Trasporto pazien- ti .Servizio infermieristico. Pulizie. Vitto. Riabilitazione	Dati anagrafici e sanitari.	Ditte e cooperative di servizi.
Legale	Conferimento incarico a studi legali esterni.	Documentazione necessaria per la predisposizione degli atti difensi- vi.	Dati personali, sanitari e giudiziari dei soggetti interessati.	Studi legali esterni.
Convenzioni	Liquidazione fatture.	Trasmissione fatture corredate dalle relative richieste.	Dati anagrafici paziente. Diagnosi, prestazione o consulenza da effettuare, motivazione della richiesta.	Strutture sanitarie convenzionate con la Fondazione o, in emergenza, anche non convenzionate.

3.1.5 Reperibilità documentazione

Tabella 5 – Ubicazione della documentazione

TIPOLOGIA	Dati sensibili e/o giudiziari	UBICAZIONE
Documentazione Sanitaria e Amministrativa in corso	Sì	- presso UU.OO.
Documentazione Sanitaria Recente	Sì	- presso UU.OO. - presso archivi della Direzione Saniataria di Presidio
Documentazione Sanitaria Remota	Sì	- presso UU.OO. - presso depositi esterni
Documentazione Amministrativa recente e remota	Sì	- presso UU.OO. - presso depositi esterni - presso ditta Italarchivi SRL
Documentazione Radiologica	Sì	- presso U.O. di Radiologia - presso archivio centrale
Documentazione Neuroradiologica	Sì	- presso U.O. di Neuroradiologia - presso archivi della Direzione Saniataria di Presidio
Documentazione Medicina Nucleare	Sì	- presso U.O. di Medicina Nucleare
Terapie infusionali personalizzate. Dialisi.File F.	Sì	- presso U.O. di Farmacia

3.2 Trattamenti con strumenti elettronici – regola 19.8

Tabella 6 – Trattamento dati di Unità Operativa Sistemi Informativi ed Informatici

Descrizione trattamento (finalità o attività)	Categoria interessati	Tipologia P: Personale S: Sensibile	Area funzionale (Struttura di riferimento)	Struttura esterna
Rilevazione presenze	Dipendenti	P	UO Personale, Direzione Sanitaria, UO non sanitarie	MondoEDP, Microntel
Contabilità, personale, approvvigionamenti, magazzini farmacia	Dipendenti e pazienti	S	Tutte le UUOO facenti capo alla direzione amministrativa, UO Farmacia	Santer (Reply)
Controllo di Gestione	Dipendenti	P	UO Controllo di Gestione	Data Processing
Stipendi	Dipendenti e borsisti	P	UO Personale, UO Amministrazione finanze	Windex
Registrazione delibere	Fondazione	P	Direzione Amministrativa	Gestito internamente
Gestione del patrimonio	Fondazione e cittadini	P	UO Patrimonio	GCS
Gestione del protocollo	Dipendenti e esterni	P	UO Protocollo	NTT Data
Accettazione, CUP, Ambulatori, Pronto Soccorso e Libera Professione	Pazienti	S	Tutte le UUOO di degenza e ambulatori, Tutte le radiologie, Direzione Sanitaria, Servizi di Pronto Soccorso, UO Controllo di Gestione	Hitech
Refertazione Ambulatoriale	Pazienti	S	Fondazione: Ambulatori Lamarmora	Hitech
Gestione dei dati di ricovero in regime di day hospital.	Pazienti	S	Fondazione	Gestito internamente
Gestione dei dati di attività di sala operatoria	Pazienti	S	Blocchi operatori della Fondazione	Gestito internamente
Dati di produzione della ricetta,	Pazienti	S	Tutte le UUOO di degenza e ambulatori, tutte le	Gestito internamente

FONDAZIONE IRCCS CA' GRANDA
OSPEDALE MAGGIORE POLICLINICO

prestazioni e farmaci			radiologie, Direzione Sanitaria	
Gestione dei dati del medico del personale	Dipendenti	S	Medico del personale della Fondazione	Gestito internamente
Gestione laboratori biochimica, microbiologia, centro trasfusionale	Pazienti	S	Tutte le strutture di laboratorio aziendali in lettura, laboratori di biochimica, microbiologia e centro trasfusionale in gestione, tutte le UUOO di degenza e ambulatori	Dedalus
Gestione dei dati di Radiologia	Pazienti	S	UO Radiologia, UO Neuroradiologia UO Medicina nucleare, tutte le UUOO di degenza e ambulatori	Fujifilm Engineering
Gestione cartella clinica del dipartimento di Patologia Neonatale	Pazienti	S	UO Terapia intensiva neonatale, UO Nido Sala Parto	I&T
Gestione emoteca e donatori per il centro trasfusionale	Pazienti	S	UO Centro trasfusionale, IEO, Centro Cardiologico Monzino, Banca dati fenotipi rari della Regione	Insiel
Gestione del coordinamento regionale dei trapianti	Pazienti	S	UO prelievo e conservazione di organi e tessuti, enti esterni afferenti all'applicativo DonorManager	Insiel Softime90
Gestione della banca del cordone ombelicale	Pazienti	S	UO Centro trasfusionale	Air Liquide H&S
Gestione referti laboratorio di Genetica Medica	Pazienti	S	UO Laboratorio Genetica Medica	Langtdev
Gestione interventi ginecologici (gestita dall'Università - corso di Laurea in	Pazienti	S	II Clinica universitaria di Ostetricia e Ginecologia	Teorema Engineering

FONDAZIONE IRCCS CA' GRANDA
OSPEDALE MAGGIORE POLICLINICO

Medicina e Chirurgia – Dipartimento di Ostetricia e Ginecologia)				
Sistema Regionale di Gestione delle psichiatrie	Pazienti	S	UO Psichiatria, Centri psico-sociali sul territorio, Servizio controllo di gestione	LI
Gestione del dato clinico padiglione Zonda	Pazienti	S	UUOO del padiglione Zonda e UUOO rianimazione Vecia	UMS (CardinalHealt)
Gestione visita e attività dei pazienti	Pazienti	S	UO di Neuropsichiatria dell'Infanzia e dell'Adolescenza	Piccolo Principe (Eurosoft-Dedalus)
Gestione immagini e dati di Neuroradiologia	Pazienti	S	UO Neuroradiologia e tutte le UUOO di degenza e ambulatori	Fujifilm Engineering
Gestione del dominio e delle relative utenze	Dipendenti ed esterni	P	UOSI	ITALTEL/NPO
Gestione dei DUMP di backup delle varie piattaforme e dei vari sistemi	Pazienti e dipendenti	S	UOSI	ITALTEL/NPO IBM/AXIOM
Gestione dei nastri e/o CD-DVDdi backup delle varie piattaforme e dei vari sistemi	Pazienti e dipendenti	S	NPO e UOSI	ITALTEL/NPO IBM/AXIOM
Gestione e controllo della navigazione Internet	Dipendenti ed eventuali esterni	S	Fabbrica Digitale, UOSI	ITALTEL/NPO
Gestione del file server di Fondazione	Pazienti e dipendenti	S	UOSI	ITALTEL/NPO
Gestione e refertazione delle immagini di Emodinamica	Pazienti	S	UO Cardiologia	Toshiba e Kardia
Immagini cardiologiche	Pazienti	S	UO Cardiologia	Medimatic
Anagrafica neonati	Pazienti	P	Servizio Centro Nascite	Intersail
Registrazioni video del sistema di videosorveglianza	Pazienti, dipendenti ed esterni	P	UOSI	Microntel Milestone
Gestione frigoemoteca	Pazienti ed esterni	S	UO Centro trasfusionale	AHSI
Gestione della	Pazienti	S	UO Nefrologia e Dialisi	Infogramma

cartella clinica per la Nefrologia e Dialisi				
Gestione pazienti emofilici	Pazienti	S	UO Ematologia	DMS Online
Gestione delle postazioni di lavoro	Dipendenti	P	UOSI	IBM/AXIOM
Gestione dati del centro trapianti fegato	Pazienti	S	UOSI e Pad. Zonda	Laboratorio di Informatica Medica
Gestione esami di laboratorio pazienti emofilici	Pazienti (anonimizzati)	S	UOS Emofilia	Ibis Informatica
Cartella informatizzata diabetologica	Pazienti	S	Day Service Ambulatoriale (DSA) UO Diabetologia	Meteda
Procreazione Medicalmente Assistita (PMA)	Pazienti	S	Centro Sterilità	ItaMedical S.r.l.
Gestione banca dati Porpora Trombotica Trombocitopenica	Pazienti	S	UO Medicina Interna	Invisible Farm

Tabella 7 – Trattamento dati di Unità Operativa Ingegneria Clinica

Descrizione trattamento (finalità o attività)	Categoria interessati	Tipologia P: Personale S: Sensibile	Area funzionale (Struttura di riferimento)	Struttura esterna
Gestione parco tecnologico apparecchiature medico-scientifiche e anagrafica ditte fornitrici	Strumentazione	P	U.O. Ingegneria Clinica	Esaote
Sistema di gestione dei tracciati cardiotocografici	Pazienti	S	Ostetricia/Ginecologia	SIDEM
Gestione immagini mammografiche Senologia	Pazienti	S	U.O. Radiologia Senologica	GMS
Sistema di acquisizione	Pazienti	S	U.O. Urologia	Olympus

e gestione immagini video e data base da sale operatorie di Urologia				
Sistema di analisi citogenetica	Pazienti	S	Laboratorio Citogenetica	Leika Microsystem
Sistema di gestione dei tracciati e referti elettrocardiografici	Pazienti	S	U.O. Cardiologia	Sylco
Sistema di acquisizione e gestione delle immagini radiologiche	Pazienti	S	U.O. Radiologia Pediatrica	GE Medical System SpA
Sistema Lambda per lettore Immunochimica	Pazienti	S	Laboratorio Immunologia Trapianti	Lagitre S.r.l.
Sistema "Gemini" per estrazione di sieri ed analizzatore di micro piastre	Pazienti	S	Laboratorio Centrale di Analisi	Pantec S.r.l.
Sistema diagnostico con piattaforma di analisi ARRAY-CGH	Pazienti	S	U.O. Laboratorio Di Genetica Medica	Agilent Technologies Italia S.p.A.
Sistema acquisizioni gestione ed elaborazione immagini radiologiche	Pazienti	S	U.O. Radiologia	Siemens
Sistema robotizzato per la preparazione di farmaci- iV Station	Pazienti	S	Terapia Intensiva Neonatale	Health Robotics
Sistema diagnostico per virologia	Pazienti	S	Laboratorio Centrale	DiaSorin SpA

Sistema "VITEK MS" per la semina automatizzata delle piastre	Pazienti	S	Laboratorio Centrale	BioMerieux Italia Spa

3.3 Progetto CRS-SISS

Trattamenti effettuati presso la Fondazione IRCCS CA' Granda Ospedale Maggiore Policlinico; misure di sicurezza adottate dall'azienda in conformità ai requisiti di legge e in conformità a quanto dispone Regione Lombardia, "contributo" dei *RESPONSABILI* designati.

Il progetto SISS è promosso e finanziato dalla Regione Lombardia per la fornitura di servizi socio-sanitari al cittadino basati sulla Carta Regionale dei Servizi.

Il progetto ha realizzato una piattaforma di servizi informatici che consente la interoperabilità e la cooperazione tra sistemi eterogenei facenti capo a soggetti diversi (Aziende Sanitarie Locali, Aziende Ospedaliere, IRCCS di diritto pubblico, Strutture Sanitarie private accreditate a contratto, Medici di Medicina Generale e Pediatri di Libera Scelta, Farmacie comunali e private) per il trattamento dei dati sanitari del cittadino.

In quanto struttura sanitaria che tratta il FSE (Fascicolo Sanitario Elettronico), la Fondazione IRCCS Ca' Granda Ospedale Maggiore Policlinico, è Titolare del trattamento.

Il progetto CRS-SISS della Fondazione è dettagliatamente descritto nei documenti di progetto i cui riferimenti vengono di seguito indicati:

- Deliberazione n. 2309 del 29 Settembre 2004 (costituzione del Gruppo Operativo Aziendale).
- Nota del 9 Novembre 2005, in atti 1219/04 all. 20 (trasmissione del documento di progetto alla Regione Lombardia).
- Nota del 24 Novembre 2005, in atti 1219/04 all. 21 (approvazione del progetto da parte della Regione Lombardia).
- I contributi della Regione Lombardia per la stesura del DPS 2013, redatti dalle Aziende Informatiche coinvolte nel SISS e designate RESPONSABILI del Trattamento dei dati personali.

3.3.1 Trattamenti di propria titolarità effettuati per finalità amministrative e di cura

I trattamenti di propria titolarità effettuati per finalità amministrative e per finalità di cura sono indicati nel documento "Contributo della Fondazione IRCCS Ca' Granda Ospedale Maggiore

Policlinico al quadro generale della sicurezza del progetto CRS-SISS", in atti 752/2000 all.52.
Misure di sicurezza adottate in conformità ai requisiti di legge e ai requisiti della Regione Lombardia
La Fondazione adotta tutte e solo le componenti standard della fornitura regionale prevista dal progetto ed in particolare dalla Piattaforma Regionale di Integrazione. Gli adempimenti specifici di competenza della Fondazione sono indicati nel documento "Contributo della Fondazione IRCCS Cà Granda Ospedale Maggiore Policlinico al quadro generale della sicurezza del progetto CRS-SISS", in atti 752/2000 all.52.

3.3.2 Contributo dei responsabili designati

I contributi relativi all'anno 2013 prodotti dalle Aziende Informatiche, nominate RESPONSABILI del trattamento dati da questa Fondazione nell'ambito del Progetto CRS-SISS, sono stati pubblicati sul sito internet www.siss.regione.lombardia.it attraverso il documento (Allegato 1 - Contributo responsabili Progetto CRS-SISS.pdf) in allegato al presente DPS.

3.3.3 OSCURAMENTO DATI

In conformità a quanto dispone il DGR VIII/5198 DEL 2/8/2007 (PROGETTO CRS - SISS).
In ottemperanza a quanto disposto dal DGR VIII/5198 del 2 agosto 2007 (Progetto CRS-SISS), la Fondazione IRCCS CA' Granda Ospedale Maggiore Policlinico ha attivato idonea procedura per l'oscuramento dei dati (P.20.F, documento del sistema qualità) in maniera da consentire all'interessato, come ulteriore e più selettivo livello di controllo sui propri dati sanitari e qualora avesse dato adesione al Fascicolo Sanitario Elettronico (FSE), la possibilità di decidere quali dati sanitari non rendere visibili (oscurare).

Gli effetti dell'oscuramento si producono solamente su istanza dell'interessato che è tenuto a presentare agli sportelli apposito modulo di "richiesta di oscuramento" predisposto dalla Fondazione. I moduli di informativa e di consenso al trattamento dei dati e gli appositi avvisi localizzati presso le casse e le sale d'aspetto, rammenteranno al pubblico la possibilità di chiedere l'oscuramento. La procedura di oscuramento può essere attivata in qualsiasi momento anche in ambulatorio e/o in reparto.

4 TRATTAMENTI DI DATI GENETICI

4.1 Provvedimenti adottati

Idonee modalità di protezione vengono adottate dai reparti ove si effettua il trattamento dei dati genetici: al personale è attribuita specifica responsabilità in merito alla custodia della parola chiave che dà accesso alle informazioni su supporto elettronico nonché al possesso delle chiavi dei locali in cui i dati genetici vengono utilizzati e conservati su supporto cartaceo. Il personale adotta comportamenti di particolare diligenza e prudenza anche durante la consegna del referto all'interessato e risulta essere adeguatamente informato dei rischi connessi al trattamento.

I dati genetici sono trattati sia con strumenti cartacei che elettronici e archiviati in banche dati elettroniche e documentali il cui accesso è controllato. Il trasferimento dei dati avviene in maniera codificata e la chiave di decodifica viene custodita in luogo separato.

Il rischio di perdita o distruzione del dato genetico è scongiurato da un sistema di duplice trascrizione: su supporto cartaceo e su supporto elettronico.

Il trattamento dei dati genetici viene effettuato in Laboratori e Padiglioni dislocati in punti diversi all'interno della Fondazione.

I dati relativi all'identità genetica vengono trattati anche presso il Padiglione Marangoni, ove ha sede il Centro Interregionale di Riferimento del Nord Italia Transplant (NITP) che raccoglie i dati dei pazienti in attesa di trapianto, dei donatori e dei pazienti trapiantati in un'area geografica che include le seguenti regioni: Lombardia, Veneto, Friuli Venezia Giulia, Liguria, Marche e la Provincia Autonoma di Trento, la Banca del Sangue Raro della Regione Lombardia (progetto di tipizzazione di 55.000 soggetti), l'archivio dei Donatori di Sangue (18.000 soggetti che donano sangue a scopo trasfusionale) e la Milano Cord Blood Bank (Banca del Sangue Placentare). Presso il Padiglione Marangoni è operativo dalle ore 21 alle ore 7 del giorno successivo il servizio di guardia armata anche a tutela dei dati ivi trattati; durante il giorno gli accessi sono controllati dal custode e in ogni caso in assenza del personale incaricato l'ingresso al padiglione dove sono custoditi i dati è chiuso a chiave. Nello stesso padiglione tutto il personale incaricato del trattamento dei dati genetici è provvisto di tesserino di riconoscimento perché possa essere facilmente identificabile. I dati genetici contenuti nella scheda riportante le caratteristiche immunologiche del sistema HLA, il gruppo sanguigno e i marcatori virali riguardanti i donatori di organi pervengono di norma dal CIR del NITP al reparto via fax (sito in

locale chiuso a chiave). I referti immunologici di compatibilità tissutale donatori probandi/riceventi pervengono al reparto in busta chiusa.

La documentazione sanitaria è custodita in armadi o contenitori chiusi presso i locali di laboratorio, il cui accesso è consentito solo al personale incaricato del trattamento dei dati genetici e viene inoltre monitorato elettronicamente tramite l'utilizzo del badge personale.

Presso il Lab. di Trombofilia i dati a titolarità diretta relativi all'utenza della Fondazione vengono acquisiti dal sistema informatico di Laboratorio (Concerto) con digitalizzazione manuale del codice esame, gli esiti vengono inseriti in Concerto e contemporaneamente viene inserito il numero progressivo di DNA che lo identifica nel programma CET consultabile dal medico referente ematologo. (Emofilia) Le provette riportano un'etichetta con Nome e Cognome e data di nascita (senza codice a barre); trascrizione dei dati anagrafici su un registro del laboratorio con numero progressivo, l'esito viene trascritto su un referto cartaceo (originale al paziente, copia in uno schedario chiuso a chiave in laboratorio, copia al medico richiedente). I dati a titolarità acquisita relativi all'utenza di strutture convenzionate e non, che richiedono prestazioni al Laboratorio specialistico di coagulazione, vengono acquisiti mediante richiesta cartacea autorizzata dalla Direzione Sanitaria della struttura titolare del dato e inseriti nel percorso comune all'utenza della Fondazione. Le richieste cartacee restano in giacenza presso il laboratorio fino al momento della fatturazione.

La necessità di migliorare la protezione dei dati genetici ha imposto un attento riesame delle modalità di trattamento in atto presso le Unità Operative, con particolare riferimento all'osservanza delle opportune precauzioni nella gestione e nella conservazione dei dati.

Operativamente ciò ha richiesto una verifica particolare presso le varie UU.OO. interessate al trattamento dove si è condotta l'analisi delle misure minime di sicurezza in atto. Gli esiti di tale verifica inducono a mantenere alto il livello di attenzione relativamente ai trattamenti in atto con interventi di verifica ulteriori che, oltre ad avere contenuti valutativi, siano anche da considerarsi momenti di approfondimento e di incontro con gli addetti ai lavori, per migliorare e perfezionare il sistema quando necessario.

Con il provvedimento del 22 febbraio 2007 "Autorizzazione generale al trattamento dei dati genetici", il Garante per la protezione dei dati personali ha inteso tutelare maggiormente l'interessato fissando regole e modalità volte a prevenire la violazione dei diritti, delle libertà fondamentali e della dignità degli interessati durante il trattamento dei dati genetici effettuati anche attraverso il prelievo e l'utilizzo di campioni biologici. Data la necessità di assicurare,

nella disciplina del trattamento dei dati genetici, un elevato livello di tutela degli stessi, la Fondazione ha provveduto a riformulare i moduli di informativa e di consenso relativi al trattamento dei dati in maniera da meglio aderire alle disposizioni date dall'Autorizzazione del Garante . L' informativa per il trattamento dei dati genetici attualmente in uso, che costituisce integrazione dell'Informativa per il trattamento dei dati personali, è il frutto dell'esame congiunto di più Enti tra cui S.I.G.U. (Società Italiana di Genetica Umana), Garante Privacy (più volte interpellato) e tutti gli interessati della Fondazione IRCCS "CA' Granda Ospedale Maggiore Policlinico" (P.18.F documento del sistema qualità).

Dopo attenta valutazione si è convenuto di predisporre una particolare procedura per l'acquisizione del consenso al trattamento dei dati genetici, alla conservazione dei campioni biologici e dei dati ad essi associati. L'intera modulistica di riferimento è stata revisionata.

L'insieme di documenti che strutturano il percorso che deve essere seguito laddove si trattino dati genetici e/o si conservino campioni biologici, costituiscono un documento che può essere utilizzato in tutto o in parte secondo le esigenze.

L'operatore sanitario che sottopone al paziente i moduli, corrispondenti alle diverse fasi di acquisizione del consenso, è tenuto a compilare e sottoscrivere la check list che costituisce un promemoria dei moduli utilizzati.

Le diverse fasi di acquisizione del consenso prevedono in primo luogo che l'operatore sanitario sottoponga all'attenzione del paziente che si presenta in ambulatorio l'informativa per il trattamento dei dati personali e l'informativa per il trattamento dei dati genetici.

Il paziente, quindi, è chiamato ad esprimere il consenso alla consulenza genetica.

Qualora il medico proponga al paziente un test genetico, si rende necessario ottenere il relativo consenso.

Nel caso al paziente venga proposta la conservazione del campione biologico, l'operatore sanitario è tenuto a raccogliere il consenso alla conservazione del campione biologico e alla conservazione dei dati sensibili e/o genetici associati.

Data la peculiarità dell'argomento, numerosi sono stati i tentativi di ottenere da parte del Garante, rassicurazioni e orientamenti precisi; allo stato dei fatti si ritiene di dover riferire la non risolta questione dei punti prelievo ematico dove ultimamente la gamma delle richieste è molto aumentata in quanto spesso vengono richiesti esami che pur essendo genetici di fatto non presuppongono un'indagine genetica specifica. Non sempre infatti i richiedenti sono consapevoli del fatto che gli accertamenti richiesti "investono" sicuramente il campo genetico

(es. la ricerca del gruppo sanguigno o i controlli per la talassemia ecc) a prescindere da una specifica richiesta di accertamento genetico.

In particolare, stante la convenzione tra la Fondazione e l'Associazione Amici del Policlinico e della Mangiagalli Donatori di Sangue Onlus, entrambi i soggetti concorrono alle attività pubbliche nell'ambito della programmazione e della legislazione Sanitaria Nazionale e Regionale e perseguono il raggiungimento degli obiettivi del piano regionale sangue e plasma. Gli accertamenti sul sangue dei donatori vengono effettuato con particolari modalità volte a evidenziare informazioni di carattere genetico, pertanto ai donatori è resa l'informativa per il trattamento dei dati genetici ai sensi dell'art.13 del D.Lgs. n.196/2003 e, prima di procedere alla donazione, il personale incaricato è tenuto a raccogliere il consenso per il trattamento dei dati genetici (M.03.515.CONS documento del sistema qualità).

4.2 Provvedimenti da adottare

Presso i laboratori di genetica permangono carenze nell'adozione delle seguenti misure di sicurezza previste per la tutela del dato genetico:

- Dati genetici e campioni biologici trattati con tecniche di cifratura.
- Trasmissione dati in formato elettronico con posta certificata
- Disgiunzione anagrafica - provetta.
- Divieto di accesso al pubblico con segreteria esterna al laboratorio.

Le misure di sicurezza idonee alla tutela dei dati genetici sono state parzialmente implementate. In particolare, in funzione della maggior tutela dei dati genetici e dei campioni biologici, le tecniche di cifratura previste per lo svolgersi del trattamento, sono attualmente da migliorare e perfezionare. Attualmente attraverso il sistema Metafora (Programma di Laboratorio: Concerto) è possibile assegnare, al momento dell'accettazione del campione biologico in Laboratorio Genetico, un codice identificativo ma sulle etichette ancora compare il nome e il cognome dell'interessato: è allo studio un sistema che permetta l'individuazione dei campioni anche se, in seguito alle recenti modifiche dell'autorizzazione del Garante al trattamento dei dati genetici, per la diagnostica non è più richiesto disgiungere la provetta dall'anagrafica: se ciò è lecito per la diagnostica rimane invece indispensabile la separazione dei dati per le finalità di ricerca. I sistemi di autenticazione per accesso ai dati sono limitati alla password che permette l'accesso all'archivio genetico. Attualmente si riscontra la non installazione di sistemi di criptatura.

L'accesso ai locali della genetica non è monitorato con sistemi biometrici. E' stata installata una elettro-serratura con un badge elettronico che abilita solo gli operatori della genetica ad entrare in laboratorio.
Attualmente la trasmissione dati in formato elettronico con posta certificata non avviene.
L'accesso del pubblico, selezionato attraverso appuntamenti telefonici e consegna referti in segreteria del laboratorio centrale, è stato organizzato in modo che non vi sia passaggio nel laboratorio di genetica.

4.3 Valutazione

Il rischio è considerato medio-alto nei Laboratori di Genetica, localizzati in punti diversi, in quanto le misure di sicurezza paiono ancora insufficienti. I processi non critici o meno critici sono quelli effettuati presso altri padiglioni come il Padiglione Marangoni dove la sicurezza è maggiore e dove il rischio è da considerarsi basso. Si ritiene importante procedere soprattutto alla criptazione dei dati, e al controllo degli accessi nei laboratori di Genetica. Il programmato trasferimento dei laboratori di genetica aumenta la probabilità di rischio nella fase di trasloco.

5 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' IN ORDINE AL TRATTAMENTO DEI DATI

(regola 19.2)

In applicazione del Codice in materia di protezione dei dati personali, la struttura privacy in ordine al trattamento dei dati all'interno della Fondazione è la seguente:

Titolare del Trattamento è il Direttore Generale della Fondazione IRCCS CA' Granda Ospedale Maggiore Policlinico: Dott. Luigi Macchi.

Responsabile interno del Trattamento dei dati è il Responsabile dell'U.O.C. Qualità, Risk Management, Appropriatezza e Privacy: Prof.ssa Silvana Castaldi. Il Responsabile del Trattamento organizza, gestisce e controlla la corretta applicazione della normativa a protezione dei dati personali e sensibili a livello aziendale.

Responsabili esterni del Trattamento dei dati sono le società indicate nelle tabelle del paragrafo 3.2 Trattamenti con strumenti elettronici – regola 19.8

Gli **Amministratori di Sistema** sono:

- → l'Ing. Alberico Bonalumi, responsabile dell'adeguamento del Sistema Informativo Aziendale (per quanto attiene i sistemi della TABELLA UOSI al paragrafo - SCHEMA DEI TRATTAMENTI DEI DATI PERSONALI - trattamenti con strumenti elettronici) alle misure minime di sicurezza e della corretta applicazione delle stesse ai sensi del D.Lgs. n.196/2003.
- → l'Ing. Gian Paolo Valente responsabile dell'adeguamento dei sistemi clinici (per quanto attiene i sistemi della TABELLA I.C. al paragrafo - SCHEMA DEI TRATTAMENTI DI DATI PERSONALI - trattamenti con strumenti elettronici) alle misure minime di sicurezza e della corretta applicazione delle stesse ai sensi del D.Lgs. n.196/2003.

I Responsabili di Unità Operativa/Servizio, hanno il compito di applicare e far applicare a tutto il personale operante nell'U.O. /Servizio di competenza, le istruzioni impartite dal Responsabile del trattamento.

Gli **Incaricati del Trattamento** sono tutti coloro che hanno necessità, per lo svolgimento delle proprie mansioni, di trattare dati. La tipologia di dati trattati da ogni incaricato è differente in funzione della specifica attività. Gli incarichi al trattamento dei dati vengono

formalizzati dal Responsabile del Trattamento che valuta, di volta in volta, l'opportunità o meno di autorizzare l'accesso ai Sistemi Informatizzati sentito anche il parere dell'Amministratore di Sistema in valutazione di fattori di opportunità e di necessità.

La rapida trasformazione dell'informatizzazione aziendale ha imposto un graduale, lento ma sistematico aggiornamento degli incarichi al trattamento dei dati con conseguente rivalutazione delle possibilità di accesso ai diversi Sistemi Informatici adottando criteri prudenziali che permettano comunque il raggiungimento di un buon livello qualitativo del processo operativo.

Per il perfezionamento degli incarichi, per tutto il 2013 e per i primi due mesi del 2014 è stata seguita una istruzione operativa d'emergenza che permetteva la gestione degli incarichi al trattamento dei dati che sono stati tutti valutati dal Responsabile del trattamento dei dati.

Al fine di rispondere con maggior efficacia al dettato legislativo e al sentito bisogno collettivo di riservatezza, in attuazione del progetto di Riorganizzazione della Struttura Privacy della Fondazione IRCCS Cà Granda Ospedale Maggiore Policlinico, è prevista l'adozione graduale di criteri organizzativi e procedurali che, in armonia con i criteri tecnici (misure fisiche ed elettroniche), devono produrre sicurezza ma anche conoscenza e assimilazione dei principi fondanti l'intera disciplina della privacy.

Le direzioni di cambiamento possono essere riassunte in quattro linee di riforma:

- il decentramento delle funzioni e delle responsabilità;
- l'istituzione di una struttura deputata al coordinamento delle attività;
- lo sviluppo della consapevolezza relativamente alla riservatezza dei dati;
- l'attenzione alle esigenze del pubblico maggiormente attento nel valutare il servizio offerto dalla Struttura Sanitaria.

Sebbene la Fondazione goda di un regime derogatorio riservato alle Pubbliche Amministrazioni, nell'Azienda Sanitaria, diversamente da altri rami della Pubblica Amministrazione, la totalità degli operatori impegnati utilizza, per l'attività di competenza, informazioni e dati relativi alla salute, pertanto l'Azienda Sanitaria Pubblica ha il compito di ottemperare diligentemente all'applicazione delle disposizioni in materia di protezione dei dati sensibili, il trattamento dei quali costituisce, per sua caratteristica strutturale, l'attività di competenza. In particolare la Fondazione, in applicazione delle disposizioni sulla riservatezza dei dati, intende compiere un ulteriore passo verso il decentramento delle responsabilità e promuove la pro-attività dei Responsabili del Trattamento.

In considerazione delle esigenze proprie della struttura complessa e della molteplicità delle attività istituzionali, il primo passo verso una riforma di carattere strutturale consiste appunto nell'affidare la Responsabilità del trattamento a più soggetti data la quantità e la diversità dei trattamenti che giornalmente vengono effettuati.

Il decentramento delle funzioni e delle responsabilità, che si inserisce pertanto nel piano programmatico di miglioramento, comporta, tra l'altro, maggiore chiarezza nella relazione con i soggetti esterni che si rapportano con la Fondazione e scoraggia comportamenti superficiali e/o scorretti, in relazione al trattamento dei dati, da parte degli operatori. I Responsabili del trattamento dei dati personali, infatti, rispondono del loro operato direttamente al Titolare. L'effetto di tale responsabilità diretta induce gli operatori a maggiore attenzione riducendo gli attuali aspetti di criticità che di norma si traducono in:

a) mancata osservanza delle procedure codificate;
b) adozione di modulistica non conforme;
c) comportamenti non autorizzati dal Titolare e/o del Responsabile del trattamento.

Seguendo un criterio quantitativo (quantità di dati trattati, quantità dei trattamenti effettuati, quantità delle Unità Operative/Servizi coinvolti nel trattamento dei dati) e qualitativo (qualità e diversità dei dati trattati) vengono individuare le tipologie di trattamento ed, in funzione delle stesse, affidate le responsabilità a coloro che sovraintendono le operazioni di trattamento dati.

Il Titolare del Trattamento è al vertice delle responsabilità nell'applicazione del "Codice in materia di protezione dei dati personali" (D.Lgs. n.196/2003) ed esercita in autonomia il potere decisionale sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Il Titolare individua e designa con atto formale il Responsabile del trattamento a livello aziendale.

Il Titolare si riserva la facoltà di nominare Responsabili del trattamento le società e le ditte esterne fornitrici di particolari servizi in outsourcing. Nel corso del 2013 è stata revisionata la procedura per la nomina del Responsabile del trattamento dei dati e per la nomina ad Amministratore di Sistema.

Compiti affidati al Responsabile del Trattamento dei dati personali interno alla Fondazione:

- procedere all'analisi dei rischi in tutti gli ambiti della Fondazione;
- redigere il Documento Programmatico sulla Sicurezza e curarne il periodico aggiornamento;

- predisporre la modulistica necessaria per l'esecuzione dei processi oggetto del trattamento da adottare all'interno della Fondazione, curarne l'aggiornamento e l'eventuale revisione in caso di necessità;
- predisporre i corsi di formazione per il personale;
- individuare momenti di comune approfondimento e verifica del percorso formativo, a scadenza periodica;
- effettuare ispezioni anche non programmate presso le UU.OO./Servizi allo scopo di verificare la corretta applicazione delle misure di sicurezza ed il rispetto dei comportamenti conformi ai principi di Tutela della Privacy;
- curare la stesura e le eventuali integrazioni del documento di Notifica al Garante.

Compiti affidati ai Responsabili di U.O./Servizio nel rispetto delle istruzioni date dal Responsabile del Trattamento:

- adempiere agli obblighi di legge per quanto attiene alla distribuzione dell'Informativa per il trattamento dei dati personali ai sensi dell'art.13 del D.Lgs. n.196/2003 e all'acquisizione del consenso degli interessati al trattamento dei dati;
- inventariare tutti i trattamenti in corso, verificandone la conformità alle vigenti disposizioni di legge e garantendo che i dati vengano trattati in modo lecito e secondo correttezza per il perseguimento delle finalità istituzionali; disporre che gli stessi non siano in eccedenza rispetto ai fini per i quali vengono raccolti o successivamente trattati; disporre altresì che siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
- curare l'adozione delle misure minime di sicurezza ai sensi del D.Lgs. n.196/2003 affinché i dati oggetto di trattamento siano adeguatamente custoditi e controllati in modo da ridurre i rischi di distruzione e di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, di comunicazione o diffusione non autorizzata;
- individuare e proporre al Responsabile del Trattamento le persone fisiche da incaricare allo svolgimento delle operazioni di trattamento stante la discrezionalità del Responsabile del Trattamento di formalizzare l'incarico in tutto o in parte. La lettera di incarico deve essere compilata correttamente indicando puntualmente l'ambito di trattamento consentito e fornendo all'incaricato le dovute istruzioni e informazioni sulle

procedure da seguire al fine di tutelare il diritto alla riservatezza e vigilare sull'accesso agli archivi e sull'integrità dei dati;

- verificare e controllare che gli incaricati si attengano alle istruzioni impartite;
- informare gli incaricati del trattamento dei dati che è vietata la creazione di nuovi archivi contenenti dati personali senza la preventiva autorizzazione del Responsabile del Trattamento;
- disporre che l'accesso agli archivi sia consentito ai soli soggetti autorizzati;
- verificare l'applicazione delle istruzioni del Responsabile del Trattamento agli incaricati affinché i documenti cartacei contenenti dati personali siano, al termine dell'orario di lavoro e comunque dopo la consultazione, riposti in luogo sicuro e ad accesso selezionato nonché predisporre appropriate misure di sicurezza per la cura e l'archiviazione della documentazione cartacea contenente dati sensibili (come ad es. referti e cartelle cliniche);
- comunicare al Responsabile del Trattamento le proposte di nuovi trattamenti e/o le modifiche di trattamenti già in atto;
- comunicare al Responsabile del Trattamento e all'Amministratore di Sistema le situazioni di rischio connesse ai trattamenti con l'ausilio di strumenti cartacei e/o informatici anche attraverso relazioni che mettano in luce eventuali carenze nel sistema;
- comunicare annualmente al Responsabile del Trattamento i rischi incombenti sui dati trattati utilizzando lo strumento del Registro Privacy;
- partecipare attivamente al processo di Formazione.

Compiti e Istruzioni affidati ai responsabili esterni del trattamento in base alla procedura di Nomina a Responsabile del trattamento della Fondazione:

COMPITI:

1. **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 rientranti nella propria sfera di competenza;
2. definire, per ciascun trattamento di dati personali, la **durata del trattamento** e la **cancellazione dei dati obsoleti**, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;

3. effettuare esclusivamente i trattamenti dei **dati personali necessari e indispensabili** all'esecuzione del presente contratto;
4. assicurare che la **comunicazione a terzi** avvenga entro i limiti stabiliti dal Titolare, ovvero, solo se autorizzata dal Titolare.
5. individuare, tra i propri collaboratori, designandoli per iscritto, gli **Incaricati** del trattamento delimitando loro l'ambito di trattamento dati;
6. mettere a disposizione del Titolare prima dell'inizio del trattamento **l'elenco del personale incaricato**;
7. curare 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;
8. 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 del Codice. In ogni caso il personale incaricato è sempre e tassativamente tenuto a comportamenti di assoluta riservatezza.
9. adottare quanto prescritto dal **disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Codice in materia di protezione dei dati personali - D.Lgs. 30 giugno 2003, n. 196;

ISTRUZIONI

A. Nel caso in cui il RESPONSABILE DEL TRATTAMENTO avesse anche funzioni di amministratore del sistema fornito, è tenuto a uniformarsi alle richieste della Fondazione in merito alla gestione degli amministratori di sistema.
B. Nel caso in cui il RESPONSABILE DEL TRATTAMENTO fosse anche l'installatore del sistema fornito, è tenuto a rispettare quanto previsto dalle politiche e dalle procedure di sicurezza della Fondazione.
C. Nel caso in cui il RESPONSABILE DEL TRATTAMENTO fosse tenuto alla consegna di un software che tratti dati personali e/o sensibili, lo stesso dovrà presentare una dichiarazione di conformità a quanto prescritto dal disciplinare tecnico in materia di misure minime di sicurezza (allegato B- D.Lgs. 30 giugno 2003, n. 196).
D. Al RESPONSABILE DEL TRATTAMENTO è fatto divieto di diffondere i dati trattati.

E. Il trattamento dei dati deve essere effettuato dal nel rispetto dei principi dettati dal D. Lgs. 30 giugno 2003 n.196 adottando tecniche di sicurezza finalizzate ad evitare rischi di indebita conoscenza da parte di terzi, perdita, manomissione, distruzione dei dati, nonché di accesso o trattamento non autorizzato.

F. Il trattamento dei dati da parte di **società in subappalto e/o consulenti** del Responsabile del Trattamento devono essere autorizzati dal Titolare pertanto lo stesso deve essere previamente informato dal Responsabile dell'esistenza di eventuali **società in subappalto e/o consulenti** che operano a qualsiasi titolo in Sua vece. Tali soggetti esterni devono comunque seguire le direttive del codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196), il disciplinare tecnico in materia di misure minime di sicurezza di cui all'allegato B del medesimo codice, il provvedimento del Garante del 27 novembre 2008 relativo a "misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008.

Compiti affidati agli incaricati:

- sono puntualmente individuati per iscritto nell'incarico che per sua stessa natura definisce l'ambito di trattamento autorizzato e le modalità di trattamento (con o senza l'utilizzo di sistemi elettronici).

6 ANALISI DEI RISCHI E DELLE CRITICITA'

L'analisi dei rischi è un importante strumento di individuazione delle più appropriate misure di sicurezza da adottare ed è quindi di supporto alle scelte per il futuro.
In materia di Tutela della Privacy i rischi e le esigenze di sicurezza diventano più significativi quando dall'ambito dei dati personali si passa a quello dei dati sensibili.
L'analisi dei rischi effettuata fa principalmente riferimento a:

- accesso non controllato ai dati conservati in forma cartacea,
- intrusione fisica ed informatica,
- indebita cognizione di dati da parte di terzi durante le attività di diagnosi e cura.

6.1 Analisi dei rischi attraverso i registri privacy

Lo strumento utilizzato per effettuare il censimento dei trattamenti in atto presso la Fondazione e l'analisi dei rischi correlati è il **REGISTRO PRIVACY** (P.22.F documento del sistema qualità).
Essendo stato l'anno 2013 un anno di transizione si chiesto ad ogni UOC/UOSD/Servizio di verificare quanto scritto nel registro privacy dell'anno 2012 e se nulla si fosse modificato di inviare una nota via posta elettronica al responsabile del trattamento dei dati per confermare quanto dichiarato nell'anno 2012. Le UOC/UOSD/Servizi in cui vi fosse state modifiche sono state invitate a redigere il registro privacy per l'anno 2013, in particolare lo si è chiesto a tutte le attività che si sono trasferite di sede.
Il pregio di tale strumento è dato dal fatto che è redatto da chi direttamente e quotidianamente si confronta con le necessità e le carenze del sistema e dell'organizzazione. Il Registro, per sua natura e struttura, permette di verificare con rapidità non solo i trattamenti effettuati presso la singola struttura ma anche i sistemi informatici utilizzati e consente agli operatori di segnalare le criticità permettendo l'analisi capillare dei rischi incombenti sui dati trattati.
Il documento REGISTRO PRIVACY di ogni UOC/UOSD/Servizio è archiviato in forma elettronica nel Documentale della Fondazione e in forma cartacea presso l'Ufficio privacy e le singole strutture. La tabella di sintesi dei rischi gravi inserita nella sez. 2 del Registro Privacy riassume le maggiori criticità evidenziando i rischi giudicati particolarmente alti denunciati dalle UOC/UOSD/Servizi.

In linea generale i rischi più frequenti giudicati alti sono dati dall'utilizzo improprio delle password cedute tra colleghi, l'utilizzo della modalità elettronica di trasmissione dei dati (la mail), l'indebita conoscenza di informazioni da parte di terzi non autorizzati e l'accesso facile ai dati cartacei conservati presso le U.U.O.O.. Nel corso del 2013 sono previste visite nuove ispettive per verificare la reale portata di tali rischi dichiarati gravi e si provvederà ad informarne la Direzione con apposita relazione.

6.2 Criticità del trattamento cartaceo

Di norma la documentazione (sanitaria e/o amministrativa) viene conservata in locali chiusi e il personale incaricato è responsabile della custodia della documentazione archiviata. Può avvenire talvolta che i dati soggetti al trattamento siano conservati negli stessi locali in cui si svolgono le attività di diagnosi e cura: in tali casi il controllo dell'accesso ai suddetti locali risulta condizionato dalla contingente necessità di svolgere l'ordinaria attività.

Per dare soluzione a tale problema era stata avviata negli ultimi anni, anche con il contributo di personale avventizio (borsisti) a ciò specificamente addetto, la costituzione di un archivio centralizzato delle cartelle cliniche. Si era provveduto altresì ad arredare, nel corso del 2004, un ulteriore archivio in località Mirasole, per le cartelle cliniche delle annate meno recenti: ivi, nel corso dell'anno 2006, è stata fatta confluire la documentazione sanitaria proveniente dall'archivio cartelle cliniche ex I.C.P. di via Maffucci e parte di quella di pertinenza del costituendo archivio centralizzato dell'ex Policlinico.

Motivazioni legate all'impossibilità di rispondere in maniera adeguata alle sopraggiunte esigenze organizzative e alla necessità di archiviare in sicurezza una quantità sempre maggiore di documentazione sanitaria hanno indotto l'Ente, tramite gara d'appalto, all'individuazione di una ditta esterna alla quale affidare la conservazione delle cartelle cliniche di tutta la Fondazione. Nel corso del 2008 alla ditta esterna è stata gradualmente consegnata la documentazione sanitaria prima depositata presso l'Archivio di Mirasole. Nei corso del 2009 è stata effettuata la consegna delle cartelle cliniche non recenti del Presidio Policlinico. Le cartelle cliniche più recenti, ancora depositate presso le varie UU.OO. e in attesa di essere catalogate, vengono temporaneamente conservate a cura dei Responsabili in appositi locali, ove possibile, o in armadi chiusi.

Al fine di ottimizzare il controllo sull'accesso alle cartelle cliniche si verifica di volta in volta, tramite personale incaricato, che la persona richiedente la consultazione e/o la consegna della cartella clinica ne abbia titolo.

Ai sensi dell'art 19 punto 5 All. B del D.Lgs.n.196/2003, in caso di danneggiamento o distruzione della documentazione cartacea recente, i dati in essa contenuti sono in parte ripristinabili perché trattati anche con strumenti elettronici ed informatici e raccolti in banche dati autorizzate.

In ogni caso nell'ambito della Fondazione è in atto un processo di informatizzazione di gran parte del materiale cartaceo esistente. Per quanto riguarda il passato (es. cartelle cliniche andate distrutte in seguito ad eventi eccezionali) alcuni dati possono essere dedotti dai registri nosologici i cui contenuti sono circoscritti al cognome e nome, alla diagnosi e alla data di ricovero e dimissione del paziente.

Nel contempo gli effetti positivi prodotti dal piano di formazione per gli incaricati del trattamento, hanno contribuito a migliorare il livello di sensibilizzazione del personale sulla questione relativa alla protezione dei dati.

Poiché la formazione è un processo permanente, sono in programma ulteriori corsi di formazione e di aggiornamento anche in funzione dell'evoluzione della normativa e della emanazione di nuove istruzioni di trattamento ai responsabili e agli incaricati; infatti solo una capillare e continua diffusione della cultura della privacy tenderà a migliorare sensibilmente il sistema e a proteggere quelle informazioni che, per loro natura, devono essere tutelate da difese sempre più adeguate.

Pur non essendosi mai verificati all'interno dell'Ente episodi di intrusione finalizzati al furto di supporti cartacei contenenti dati personali, il livello di rischio è da considerarsi medio data l'elevata frequenza di furti di apparecchiature informatiche e di altre attrezzature di elevato valore commerciale.

Al fine di abbassare il livello del rischio si è provveduto ad installare, ove possibile, sistemi per la messa in sicurezza dei locali e delle apparecchiature.

In particolare sono state installate:

- porte blindate, quando possibile;
- serrature rinforzate e/o di sicurezza;
- pesanti catene con lucchetti ai computer come antifurto;
- accesso ai reparti tramite codice numerico (Pad. Monteggia – Pad. Zonda – De Marchi).

E' stato sensibilizzato tutto il personale affinché porte e finestre siano ben chiuse alla fine dell'orario di lavoro ed è stato allertato il personale di portineria, soprattutto quello dei turni di notte.

Le attività di diagnosi e cura presso tutte le Unità Operative comportano colloqui tra medici e pazienti. Il rischio di indebita conoscenza da parte di terzi di dati sensibili è quindi presente.
Al fine di abbassare il livello di rischio nei luoghi preposti alla diagnosi e alla cura, dove spesso è altresì difficile assicurare la privacy del paziente se non con modalità che influirebbero pesantemente sulla celerità e/o efficacia delle attività svolte, si è cercato di aumentare il livello di attenzione dei responsabili e degli incaricati.
A tale proposito, si è provveduto ad adottare idonee misure per garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati. Nella fattispecie sono state istituite appropriate distanze di cortesia nei locali CUP e negli ambulatori, là dove la struttura del locale lo rendeva possibile, posizionando a terra strisce gialle ben visibili.
Il programma di riassetto organizzativo della Fondazione ha altresì previsto la produzione di nuova modulistica. In particolare sono state previste procedure per informare i terzi legittimati sulla dislocazione dei pazienti ricoverati nell'ambito dei reparti rispettando le volontà degli interessati in relazione alle occasioni di visita.
La formazione del personale è strutturata in modo utile a prevenire eventi tali per cui persone estranee e quindi non legittimate possano venire a conoscenza dei dati dell'interessato o porre in correlazione l'interessato con specifici reparti o strutture.
Sempre nell'ambito dei corsi di formazione è in atto una continua sensibilizzazione del personale al rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dati.
L'analisi dei trattamenti effettuati con l'ausilio di strumenti informatici è trattata nel paragrafo 3.2 e nel paragrafo 6.4.

6.3 Criticità dell'attuale struttura privacy

Stante la struttura complessa dell'Azienda Sanitaria, le complicate decisioni in ordine alla privacy devono poter essere assunte con maggiore consapevolezza dagli operatori e quindi tendere all'ottimizzazione delle modalità di gestione dei dati personali.
Pertanto, in attuazione del progetto di riorganizzazione della struttura privacy della Fondazione che prevede il decentramento della responsabilità del trattamento, i nominati Responsabili del trattamento dei dati personali (interni ed esterni alla Fondazione) sono chiamati a rispondere del loro operato direttamente al Titolare.
Tale responsabilità diretta induce gli operatori a maggiore attenzione riducendo gli attuali aspetti di criticità emergenti:

a) la mancata osservanza delle procedure. In particolare si rileva che la procedura di " Nomina a responsabile del trattamento esterno" (es ditte in outsourcing) è stata solo parzialmente recepita nonostante le sessioni di formazione appositamente organizzate nel 2011 e nel 2012 per la presentazione della procedura ai Responsabili di UOC/UOSD/Servizio che, per le competenze del proprio ufficio, sono tenuti ad utilizzarla.
La mancata acquisizione da parte della Fondazione dei Registri Privacy dei Responsabili Esterni è ulteriore sintomo del marcato disinteresse reciproco (degli organi preposti della Fondazione da una parte e delle ditte in outsourcing dall'altra) per l'attività di verifica e controllo sulle operazioni di trattamento.
Sempre ai fini di trasparenza è auspicabile che la sottoscrizione di contratti e/o convenzioni con soggetti esterni venga resa nota al Responsabile del Trattamento adottando soluzioni uniformi per tutte le strutture della Fondazione già proposte dalla procedura di riferimento e ancora purtroppo disattese.
b) La frammentazione della modulistica e/o l'uso di modulistica non conforme a quella codificata in Fondazione e quindi non autorizzata dal Responsabile del trattamento interno della Fondazione è un problema reale che si ripercuote, nella pratica quotidiana e che insidia il sistema privacy. In particolare si fa riferimento:
- al modulo, attualmente a sistema, di consenso al trattamento dei dati per i pazienti. Nel corso del tempo l'Ufficio Privacy ha invano richiesto più e più volte che la formula di consenso proposta ai pazienti fosse quella emessa dallo stesso ufficio e non altra.
- al modulo di informativa per il trattamento dei dati che ancora non risulta a sistema e conseguentemente non viene direttamente consegnato agli interessati che ne possono solo prendere visione presso le sale d'aspetto nelle aree cassa e ambulatori dove l'informativa è affissa a parete. Si considera indispensabile adottare quanto prima una modalità corretta per informare il pubblico del trattamento dei dati dato che alle casse il modulo di informativa non viene consegnato brevi manu all'interessato nonostante l'Ufficio privacy ne abbia più volte sottolineato la necessità.
c) Le attività e le iniziative autogestite dalle U.U.O.O. in ordine al trattamento dati senza previa autorizzazione del Responsabile del trattamento interno dei dati della Fondazione produce grave pregiudizio al sistema privacy (es. trasmissione non autorizzata di dati sensibili a mezzo posta elettronica) inducendo perfino a considerare infruttuoso il compito del Responsabile del trattamento di accrescere in Fondazione la cultura della riservatezza.

d) La circolazione delle informazioni all'interno e all'esterno della Fondazione attualmente ancora non risponde ai requisiti di sicurezza richiesti. Si è riscontrato infatti, anche recentemente, la non aderenza alle politiche di sicurezza della Fondazione in ordine alla trasmissione dei dati personali e delle informazioni. Nell'occasione di stabilire, per il futuro, un modus operandi aderente alla policy della sicurezza, già pubblicata nell'internet della Fondazione, è stata richiamata la necessità di evitare comportamenti che potrebbero arrecare pregiudizio all'integrità dei dati e che potrebbero consentire l'indebita conoscenza da parte di terzi.

6.4 Criticità dell'attuale sistema informativo

Da un'attenta analisi del sistema informativo, le aree risultate di maggiore criticità in riferimento ai trattamenti effettuati digitalmente sono quelle descritte nei paragrafi seguenti.

6.4.1 Rischi connessi alla non disponibilità della rete interna della Fondazione

Per il controllo-gestione della rete è stato attivato un servizio di presidio e di helpdesk in outsourcing che si basa su:

- attivazione di un servizio di helpdesk con numero telefonico dedicato (59999) presidiato dal lunedì al venerdì dalle 8.30 alle 18.00;
- utilizzo del numero verde Telecom 800209985 in tutti gli altri orari e giorni (24x7) attivabile dal personale del centralino o dal referente della Direzione Sanitaria.

La Fondazione ha realizzato un progetto di revisione della topologia di rete interna (fibra a 10Gbit/s) finalizzata:

- all'eliminazione dei singoli percorsi di rete sia tra padiglioni, sia all'interno della connettività del Data Center principale, in modo da scongiurare la possibilità del "single point of failure"
- alla sostituzione degli apparati di core con una nuova, performante e più affidabile tecnologia

Per completare quanto già effettuato sulla rete e raggiungere un adeguato livello di sicurezza sarà fondamentale effettuare:

1. la sostituzione degli apparati di accesso alle varie utenze con la stessa tecnologia utilizzata nei core ➔ maggiore gestibilità, maggiore performance e maggiore sicurezza

2. lo spostamento graduale degli armadi di rete posizionati in corridoio o in stanze soggette ad accesso esterno → maggiore sicurezza (diminuzione di sabotaggi o di rischi connessi ad azioni maldestre) e conseguente innalzamento della disponibilità dei servizi
3. tutte quelle opere preparatorie al previsto abbattimento dei padiglioni per evitare di isolare intere zone della Fondazione

6.4.2 Rischi connessi alla connettività di reti esterne alla Fondazione

I collegamenti esterni si basano su una soluzione di doppia connettività internet basata su un collegamento a banda larga secondo le modalità e le specifiche previste dalla convenzione Consip – Fastweb e su un collegamento anch'esso a banda larga con la rete universitaria Garr; tali servizi sono configurati per ottenere elevati standard di continuità e di performance.
In particolare la connettività Fastweb prevede un accesso dedicato ad Internet tramite profilo SDH 20 Mbit/s con una banda minima garantita di 18.4 Mbit/s sia in upload che in download, l'operazione di nat fra i 32 ip pubblici assegnati e la rete interna, la gestione del servizio di Firewall su questa linea.
Sono oltremodo possibili soluzioni di collegamento tra sedi diverse in grado di soddisfare tutte le esigenze di comunicazione sia per i dati che per la fonia mediante il carrier Fastweb; allo scopo è presente presso la sede di via Sforza una ulteriore connessione SDH 10 Mbit/s a cui afferiscono ad oggi 8 sedi periferiche.
La seconda connettività si basa su una linea ethernet in fibra ottica a 100 Mbit/s afferente alla rete universitaria Garr, attraverso la quale è erogata l'ulteriore connettività internet. La linea è attestata su un router Cisco 2821 gestito direttamente dalla Fondazione; questo apparato effettua il routing della lan di 256 ip pubblici assegnati alla Fondazione. Le operazioni di controllo degli accessi e di NAT sono effettuati da un firewall Cisco Pix 515E (in fase di duplicazione per massima affidabilità nel primo semestre 2008), gestito direttamente dalla Fondazione.
Su detto firewall è attestata inoltre tutta la connettività relativa al progetto regionale SISS: il relativo traffico di rete è stato analizzato congiuntamente ai tecnici SISS e sulla base degli accordi intercorsi sono state adottate le relative regole di attraversamento che limitano il traffico a quanto strettamente indispensabile per il corretto funzionamento del servizio.
Il medesimo firewall opera anche da gestore della zona demilitarizzata (DMZ) nella quale sono posizionati i server relativi alla rete regionale ed interregionale Nitp e al sistema per la Libera

Professione Ospedaliera. Detti sistemi sono protetti a livello di firewall da tutto il traffico non autorizzato, esponendo al contempo i servizi strettamente necessari al funzionamento del sistema.

E' inoltre presente un servizio in Hosting presso Fabbrica Digitale (subappalto del contratto ITALTEL/NPO) della piattaforma Web Server e Mail Server, in maniera tale da garantire i migliori livelli di disponibilità e continuità.

In aggiunta a quanto detto, sono stati adottati i seguenti provvedimenti:

- implementazione di un proxy per consentire una navigazione filtrata e controllata,
- configurazione del sistema firewall con regole restrittive.

Per raggiungere un adeguato livello di sicurezza sarà fondamentale effettuare:

1. l'aggiornamento del sistema firewall in favore di una tecnologia decisamente più moderna → maggiore sicurezza e maggiore controllo dovuti alle nuove tecnologie ed alle maggiori possibilità offerte dai nuovi prodotti di firewalling.
2. l'implementazione di un sistema IPS (Intrusion Prevention System) per prevenire attacchi esterni e proteggere adeguatamente i dati del sistema informativo
3. il rinnovo del sistema di VPN con cui si collegano i vari enti esterni → utilizzo di una tecnologia più idonea a controllare meglio le azioni di chi si inserisce nella rete interna dall'esterno (fornitori, partner, altri ospedali...)
4. il rinnovo e l'ottimizzazione del sistema proxy per poter navigare in maniera maggiormente sicura e per permettere una maggiore possibilità di visione agli utenti

6.4.3 Rischi connessi agli impianti dei data-center della Fondazione

La Fondazione dispone complessivamente dei seguenti locali tecnici adibiti a data-center:

- sala macchine palazzina uffici di via Sforza (datacenter principale);
- sala macchine padiglione Devoto (datacenter secondario);
- sala macchine centro trasfusionale presso padiglione Marangoni;

Tutti i locali adibiti a data center sono provvisti di gruppo di continuità, rilevatore anti-fumo/anti-incendio e impianti di condizionamento.

I gruppi di continuità e il gruppo elettrogeno sono stati ulteriormente revisionati e messi sotto monitoraggio dall'U.O. Funzioni tecniche.

E' stato realizzato un sistema di controllo accessi, rilevazione fumi, rilevazione presenze, rilevazione temperatura e videosorveglianza.

Per ottimizzare e completare il sistema virtuale implementato nel datacenter secondario (Devoto) è importante:

1. acquistare nuovi server aggiuntivi da affiancare all'unico nodo ESX di Palazzo Uffici ad integrazione della parte virtuale → completamento del progetto di disaster recovery e di conseguenza raggiungimento della piena funzionalità dello stesso
2. l'utilizzo di un dispositivo più adeguato alla mole di traffico ed alle esigenze di controllo nella sala CED 2 (Padiglione Devoto) → maggiore disponibilità della rete e maggiore efficienza nell'eventuale ripristino del servizio (in caso di disaster recovery)

6.4.4 Rischi connessi all'indisponibilità dei sistemi server

Tutti i server dedicati alle applicazioni sono in configurazioni ridondate in modo da replicare il più possibile i dispositivi soggetti a guasti ed evitare così di avere "single point of failure".
Per la configurazione dettagliata di ciascun server fare riferimento alla procedura del sistema qualità P.04.050 Procedura di gestione del sistema informativo.
Tutti i sistemi sono in configurazione ad alta affidabilità, vale a dire prevedono tutti gli elementi di ridondanza tali da garantire la continuità di funzionamento anche in caso di guasto di uno o più componenti.
Nel corso del 2008 è stato attivato il sistema di controllo automatico Nagios che informa anche via SMS gli operatori della UO Sistemi Informativi in modo proattivo sullo stato di criticità dei server.
L'indicatore di qualità relativo alla disponibilità dei sistemi è molto buono, nel corso del 2011 non si sono avuti incidenti significativi, fatto salvo tutti quelli programmati ed aventi lo scopo di rinnovare la rete con i nuovi dispositivi. Il livello di uptime è monitorato dal sistema qualità.
Occorre nel futuro provvedere all'installazione di sistemi server secondari, presso il datacenter secondario (Devoto), da attivare in caso di indisponibilità dei sistemi server primari.

6.4.5 Rischi connessi a virus informatici

Tutte le postazioni di lavoro sono dotate di software antivirus Symantec con aggiornamento automatico delle definizioni e con installazione automatica delle patch di sicurezza del sistema operativo.
Dove possibile tecnicamente, ovvero nelle postazioni di lavoro nuove, sono state attivaste tutte le componenti del prodotto: anti-virus-malware, anti-spyware e personal firewall.

La distribuzione automatica del sistema antivirus raggiunge ormai la totalità delle postazioni di lavoro. La presenza di virus è monitorata centralmente dal servizio di fleet management: sono disponibili presso l'UO Sistemi Informativi i documenti di assessment periodici della situazione che risulta essere molto positiva.
Il sistema di distribuzione automatica dell'antivirus e della patch di sicurezza del sistema operativo consente un monitoraggio continuo ed automatico dello stato delle protezioni antivirus.
Con l'arrivo auspicato di postazioni nuove in sostituzione delle obsolete, verranno attivate su un maggior numero di postazioni di lavoro le nuove funzionalità rese disponibili dal software.

6.4.6 Rischi connessi all'accesso ai sistemi informativi

Un primo livello di protezione è garantito dall'accesso alle stazioni di lavoro che avviene con inserimento di un account utente individuale i cui diritti ed autorizzazioni sono stabiliti nel server di dominio centrale. Sono stati definiti, e vengono applicati per tutti i nuovi collegamenti alla rete, alcuni criteri minimali quali:

- password obbligatoria e cambiata automaticamente ogni 3 mesi;
- password manutentiva per il profilo administrator noto solo al personale dell'U.O. Sistemi Informativi ed ai gestori ITALTEL/NPO e IBM/AXIOM;
- nessun utente comune con diritti di administrator.

Un secondo livello di protezione avviene a livello dei programmi applicativi, che sono resi accessibili agli operatori soltanto dopo l'esito positivo della procedura di autenticazione (codice identificativo *User-ID* e di una parola chiave riservata *password*); il superamento della fase di autenticazione abilita gli operatori all'esecuzione delle funzioni a cui essi sono stati preventivamente autorizzati secondo i profili definiti nell'ambito di ciascun applicativo.
Durante i corsi di addestramento sugli applicativi, i tecnici formatori si soffermano sull'importanza di una corretta gestione di User-ID e password. Le password vengono assegnate dal servizio di fleet management e, successivamente, possono essere modificate a cura dei singoli utenti. Il codice per l'identificazione è univoco e non può essere duplicato: non è possibile, cioè, assegnare a due utenti diversi il medesimo codice identificativo.
L'attribuzione di un profilo di autorizzazione ad un utente avviene sulla base dell'incarico assegnato dal responsabile dell'Unità Operativa che gestisce il trattamento attraverso funzioni proprie dell'Amministratore del Sistema.

Sono stati forzati alcuni automatismi sulla verifica sintattica delle password e sulla loro scadenza in modo da rendere intrinsecamente sicuro il processo e alleggerire le procedure di gestione. Tutte le regole di attivazione e gestione delle credenziali sono state definite e divulgate attraverso le politiche della Fondazione: in questo caso la politica di gestione delle password, reperibile dalla intranet aziendale come tutte le altre.

Il processo di assegnazione degli incarichi è stato formalizzato così come la richiesta e la revoca di accesso al sistema informativo attraverso apposita richiesta del responsabile di UO:

- all'informatica per tutti quegli applicativi che NON trattano dati sensibili,
- al sistema digitale della privacy per tutti quegli applicativi che trattano dati sensibili.

E' a disposizione degli utenti un servizio di helpdesk attivo 24h per assistere gli utenti nella gestione delle credenziali di accesso per evitare che gli automatismi imposti blocchino le attività.

Devono ancora essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Le attività fortemente consigliate in ottica miglioramento sono le seguenti:

1. richiedere ai fornitori applicativi di rendere i propri software integrabili con il nostro dominio affinché diminuiscano sensibilmente le credenziali che gli utenti devono gestire
2. ottimizzare la struttura del nostro dominio, migrandolo alla versione 2008 e gestendolo in maniera più precisa e sicura
3. rivedere tutte le politiche di sicurezza impostate a livello centrale

6.4.7 Rischi connessi ad accessi interni non autorizzati

Il controllo dell'accesso al sistema informativo secondo le modalità esposte al paragrafo precedente riduce la possibilità per un utente interno alla rete aziendale di accedere, senza autorizzazione, ai dati conservati su apparecchi collegati alla rete stessa a patto che gli utenti mantengano riservate le credenziali di accesso. Nell'ambito dei corsi di formazione questa importante responsabilità viene molto evidenziata e vengono ricordati i comportamenti da

evitare (es. scrivere le password su documenti facilmente accessibili). Il processo di assegnazione formale dell'incarico implica una presa di responsabilità.

L'aderenza a quanto definito viene controllata mediante:

- monitoraggio dei sistemi
- verifiche ispettive nei luoghi di lavoro

Tutti i responsabili di Unità Operativa sono stati sensibilizzati a vigilare sul comportamento degli utenti e a comunicare comportamenti non corretti.

Per raggiungere un migliore livello di sicurezza sarà fondamentale effettuare:

1. l'implementazione di un sistema IPS (Intrusion Prevention System) per prevenire attacchi interni e proteggere adeguatamente i dati del sistema informativo
2. l'esecuzione di test che verifichino lo stato di aggiornamento del sistema e la rispondenza alle politiche di sicurezza definite
3. la sperimentazione, nell'ambito del progetto SISS, l'autenticazione degli utenti del sistema informativo attraverso smart card

6.4.8 Rischi connessi a spamming, phishing o altre tecniche di sabotaggio

E' stato implementato sul server di posta elettronica un servizio di filtro anti-spam che limita notevolmente l'arrivo di mail pericolose nelle caselle degli utenti finali.

L'efficacia del filtro anti-spam è:

- verificata continuamente dall'amministratore di sistema che rileva ogni eventuali traffico anomalo dovuto all'incremento del numero di messaggi,
- garantita dall'aggiornamento del sistema di verifica delle signature di rilevamento delle mail considerate pericolose.

Il notevole aumento della richiesta di caselle di posta impone l'acquisto di ulteriori caselle di posta ed un servizio di gestione più efficace ed efficiente: senza questo presupposto il sistema informativo non è in grado di soddisfare la richiesta interna.

Sarebbe opportuno richiedere al fornitore che l'autenticazione alle caselle di posta avvenga in integrazione con il nostro dominio centrale affinché si possa togliere all'utente finale anche la gestione delle relative credenziali.

6.4.9 Rischi connessi a intercettazione di informazioni in rete

Si tratta della possibilità per un utente di accedere ad informazioni riservate mediante collegamento non autorizzato alla rete aziendale, intercettando informazioni a lui non destinate.

E' stato installato un sistema di sicurezza per dotare tutti gli armadi di rete di un sensore di porta aperta in modo tale da monitorare attraverso una centrale operativa allarmi ogni tentativo di apertura.

Per le postazioni di lavoro installate presso la Fondazione la password di amministratore, necessaria per l'installazione di programmi di sniffing del traffico, non è nota agli utenti che pertanto non possono dotarsi di tali programmi.

E' stato inoltre installato il programma LanDesk per il controllo remoto del software installato sulle postazioni di lavoro in modo tale da monitorare l'installazione di software non autorizzato.

Sui sistemi server viene attivato l'audit automatico per monitorare tentativi di accesso e conseguente attivazione di uno script per la trasmissione di un messaggio di allerta al servizio di help desk attivo 24x7 (tutti i giorni 24 ore su 24); il servizio di help desk, in caso di ripetuti tentativi di accesso, è autorizzato a bloccare l'accesso al server.

E' stato attivato un sistema di distribuzione automatica delle patch di sicurezza per le postazioni di lavoro.

E' stata attivata l'infrastruttura per predisporre l'associazione tra la porta di connessione degli apparati di rete e l'indirizzo fisico della scheda di rete delle postazioni di lavoro in modo tale da bloccare il collegamento di postazioni di lavoro non autorizzate.

Per migliorare sensibilmente questo punto molto delicato ed eccessivamente rischioso per la Fondazione occorre necessariamente:

1. sostituire tutti gli armadi di rete rotti e quindi facilmente accessibili da sabotatori
2. sistemare tutti gli armadi non rotti ma che rendono semplice l'accesso ai cavi (spesso a vista)
3. uniformare le serrature di tutti gli armadi riparando anche i contatti non più funzionanti
4. coprire con un adeguato cavedio i cavi esterni lasciati scoperti come ad esempio quello relativo alla sala CED del Granelli
5. implementare un valido sistema di blocco a livello rete di utenti non riconosciuti (802.1x – progetto NAC, ovvero Network Access Control)

6. affidare a personale dedicato il monitoring degli allarmi, attualmente in carico alle portinerie

6.4.10 Rischi connessi ad esportazione e furto di strumenti contenenti dati

Ovvero furto di personal computer, server, supporti rimuovibili per i backup, dischi esterni, etc...

E' stato installato un sistema per il controllo accessi dei locali adibiti a datacenter. Il progetto prevede anche l'installazione di sensori di presenza collegati a una centrale di monitoraggio allarmi attiva 24h. E' inoltre attivo per il datacenter Sforza un sistema di videosorveglianza.

Tutti i media di backup sono custoditi in una cassaforte ignifuga.

Nell'ambito dei corsi di formazione gli utenti vengono resi consapevoli dei rischi relativi alla memorizzazione dei dati sugli hard disk delle stazioni di lavoro.

Agli utenti che ne fanno richiesta viene installato un modulo per la crittografia dei file.

E' stato implementato nel 2011 un nuovo servizio di file server basato su tecnologia di criptazione trasparente all'utente: si tratta di un server che eroga delle share di rete disponibili ad ogni UO ed in cui il personale inserisce i propri dati sensibili evitando di lasciarli sulla propria postazione. In maniera trasparente agli utenti, questi dati sono memorizzati su un sistema di storage criptato.

E' stato fatto un procedimento di estensione per controllare tutti gli ingressi principali ai padiglioni sia con telecamera che con sensore di apertura porta.

Il rischio di furto è alto soprattutto presso i padiglioni non presidiati della Fondazione. La presenza di numerosi cantieri aumenta ulteriormente il rischio. Considerando il pericolo per la Fondazione derivante da questa tipologia di rischio, occorre in futuro:

1. completare il documentale criptato affinché sia disponibile a tutte le UO, riesca a contenere tutto quanto richiesto, sia efficacemente soggetto a backup e maggiormente fruibile alle utenze
2. migliorare il sistema di videosorveglianza, decisamente obsoleto, che rende il sistema ingestibile e difficilmente utilizzabile: le immagini richieste vengono spesso perse, consegnate in ritardo e sono inutilizzabili data la scarsa risoluzione delle videocamere
3. dotare di apriporta con badge le sale CED non provviste come ad esempio il Granelli

7 CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI

(regola 19.5)

7.1 Strategia di backup

Per ognuna delle banche dati aziendali è stata individuata una modalità di creazione dei backup e di verifica degli stessi. Allo stesso modo, sono stati definiti i criteri e le condizioni necessarie per l'utilizzo degli stessi.

Procedura di backup: procedura giornaliera di export dal database Oracle e memorizzazione su SAN/DAT. Il backup su disco è configurato in maniera tale da conservare le copie dei 3 giorni precedenti: le copie più vecchie vengono sovrascritte.

Procedura di verifica della disponibilità dei dati per il ripristino: verifica dei log Oracle e registrazione sul registro giornaliero dei backup.

La banca dati Paghe (Aliseo) è gestita direttamente dalla società Windex nell'ambito del contratto di esternalizzazione del servizio.

Tutti i trattamenti dati effettuati su server centralizzati sono sottoposti a politica di backup stabilita dal Responsabile del servizio informatico che deve prevedere una periodicità non inferiore alla settimana per l'esecuzione.

Allo stato attuale, i backup centralizzati sono eseguiti giornalmente.

Tutti i supporti di backup sono conservati in luogo sicuro e ad accesso selezionato.

I trattamenti non centralizzati e comunque tutti quelli locali sono a carico della UO di riferimento e dei relativi Responsabili del Servizio che ne controllano l'avvenuta operazione di backup con periodicità non superiore alla settimana.

7.2 Strategia di disaster recovery: l'infrastruttura virtuale

L' infrastruttura virtuale è composta da due siti ubicati in edifici diversi. Il Sito SS2 (CED del padiglione Devoto) si compone di 5 host IBM 3850M2. Nel sito SS1 (CED di Palazzo Uffici) è presente un solo host IBM3850M2. In tutti gli host è stato installato VMware ESXi ver. 4.0 U1. La funzione di vCenter -ver 4.0 U1- per la gestione dei 6 host è affidata ad una VM dotata di sistema operativo Win2008 Std 64bit in cui è installato anche Sql server 2008 Standard 64bit.

8 INTERVENTI FORMATIVI PER IL TRATTAMENTO DEI DATI

(regola 19.6)

L'intervento formativo degli incaricati al trattamento risulta essere essenziale supporto al programma di sicurezza della struttura.

La formazione è un processo permanente che all'interno della Fondazione si sviluppa nel rispetto di un piano articolato in più incontri programmati nell'arco dell'anno in maniera da adattarsi alla disponibilità di tempo dell'incaricato che continua a svolgere la sua normale attività e soprattutto in considerazione anche dell'evoluzione normativa e dell'emanazione di nuove istruzioni di trattamento ai responsabili e agli incaricati.

L'Amministratore di Sistema e il Responsabile del trattamento erogano periodicamente corsi di formazione base dal titolo: "Trattamento dei dati sanitari e misure di sicurezza".

I corsi, più volte riproposti nel corso dell'anno, sono diretti ai Responsabili di Unità Operativa/Servizi e agli incaricati dei trattamenti dei dati personali. I Responsabili di Unità Operativa/Servizi replicano le sessioni formative all'interno della propria organizzazione utilizzando gli strumenti didattici messi a loro disposizione.

La partecipazione ai corsi è obbligatoria per i Responsabili di Unità Operativa/Servizi e per gli incaricati ed è registrata presso il Responsabile del Trattamento: per i Responsabili di Unità Operativa/Servizi è prevista la possibilità di conferire una delega. Ai partecipanti viene rilasciato un certificato di frequenza firmato dal Responsabile del Trattamento.

Sessioni di training sono state organizzate nelle UU.OO. al fine di approfondire particolari la trattazione di particolari ambiti in materia di trattamento dei dati personali (es. presso il centro sterilità ed il centro donatori del sangue dove si è affrontato il tema del trattamento dei dati genetici).

Si è reso altresì necessario approfondire le tematiche del sistema privacy anche dialogando con interlocutori esterni alla Fondazione (Comune di Milano altri Ospedali).

Nell'Intranet della Fondazione, come lo è stato sempre nel passato, il corso privacy rivolto a tutti gli operatori dal titolo: "*Trattamento dei dati sanitari e misure di sicurezza*".