FONDAZIONE I.R.C.C.S.
ISTITUTO NEUROLOGICO CARLO BESTA

Fondazione IRCCS Istituto Neurologico "Carlo Besta"

Documento programmatico sulla sicurezza dei dati (DPS)

***

Aggiornamento 2011

Sistema Sanitario Regione Lombardia

Fondazione I.R.C.C.S. Istituto Neurologico Carlo Besta
Via Celoria 11, 20133 Milano - Tel 02 2394 1 - CF 01668320151 - PI 04376340156 - www.istituto-besta.it

INDICE

§ 1 Premessa

Vista la normativa in materia di trattamento di dati personali ed in particolare:

- il Decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali);
- il Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B);

la Fondazione IRCCS Istituto Neurologico "Carlo Besta", in qualità di Titolare del trattamento dei dati, provvede alla revisione del ***Documento Programmatico Sulla Sicurezza dei dati (DPS).***

Il presente Documento Programmatico sulla sicurezza dei dati, aggiorna integralmente il DPS adottato con Deliberazione n. 130 del 31 Marzo 2010 ed ha lo scopo di illustrare le misure minime di sicurezza attraverso le quali la Fondazione, **Titolare** delle operazioni di trattamento, in considerazione della tipologia dei dati trattati, protegge il proprio patrimonio informativo.

Il documento contiene tutte le informazioni richieste dal punto 19) **del Disciplinare Tecnico.**

§ 2 Elenco dei trattamenti di dati personali (19.1)

Conformemente a quanto disposto dal punto 19.1 del Disciplinare Tecnico si è provveduto ad individuare l'elenco dei trattamenti di dati personali mediante: a) la descrizione dei trattamenti effettuati dalla Fondazione in conformità anche a quanto indicato nel Regolamento Regionale n. 9 del 18 luglio 2006 per il trattamento dei dati sensibili e giudiziari; b) l'individuazione dei tipi di dati personali oggetto dei trattamenti stessi.

- **Operazioni standard:**

Raccolta (acquisizione verbale e/o documentale diretta o indiretta, acquisizione informatica da archivi regionali o da altri soggetti esterni) elaborazione diretta, registrazione, aggregazione, organizzazione, consultazione, modificazione, selezione, estrazione, raffronto, utilizzo, trasformazione in forma anonima, blocco, conservazione, distruzione, cancellazione.

- **Operazioni particolari:**

1) Interconnessioni con altri trattamenti o archivi (altre Aziende Sanitarie od Ospedaliere, archivi relativi alle prestazioni, anagrafe regionale assistiti, Ministero della Salute, ISTAT, Regione Lombardia, Istituto Superiore della Sanità).

2) Comunicazioni di dati con interessato identificabile (es. esercenti la patria potestà, enti previdenziali, autorità giudiziaria, organi di controllo, organizzazioni sindacali, Presidenza del Consiglio dei Ministri- Dip. Funzione Pubblica, Forze dell'ordine, Compagnie di assicurazione, ASL, ed altri Enti destinatari per legge o per regolamento).

Tali operazioni di trattamento possono avere ad oggetto dati personali, sensibili, genetici e giudiziari, la cui titolarità è in capo alla Fondazione:

- **Dati personali**

Informazioni relative a, persone fisiche, persone giuridiche, enti od associazioni, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero d'identificazione personale (*ex lettera b) art.4 D.lgs n.196 del 30 giugno 2003*).

Nello specifico dati relativi a persone fisiche e persone giuridiche in rapporto con la Fondazione:

- pazienti
- personale dipendente
- personale non strutturato (borsisti, collaboratori, tirocinanti, frequentatori, altro)
- clienti
- fornitori.

- **Dati sensibili**

Dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (*ex lettera d) art.4 D.lgs n.196 del 30 giugno 2003*).

Nello specifico, cartelle cliniche di ricovero, diari clinici, registri nosologici, registri delle prenotazioni, schede di dimissione ospedaliera, relazioni cliniche, archivi di attività diagnostiche/terapeutiche (impegnative, ricevute di ticket, cartelle ambulatoriali, referti, lastre), registri di sala operatoria, dei decessi, delle autopsie, registri e documenti relativi alle sperimentazioni cliniche, dati relativi alle donazioni, accertamenti relativi all'idoneità lavorativa, dati

idonei a rivelare il comportamento sessuale, schede personali relative all'iscrizione ai sindacati, curriculum vitae, fascicoli del personale dipendente.

- **Dati genetici**

I dati che, indipendentemente dalla tipologia, riguardano la costituzione genotipica di un individuo, ovvero i caratteri genetici trasmissibili nell'ambito di un gruppo di individui legati da vincoli di parentela il cui trattamento è stato oggetto di un'autorizzazione specifica (22 febbraio 2007) da parte del Garante privacy.

- **Dati giudiziari**

Dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale (*ex lettera e) art.4 D.lgs n.196 del 30 giugno 2003*).

Tali operazioni di trattamento vengono svolte dalla Fondazione IRCCS Istituto Neurologico "Carlo Besta", nell'esercizio dell'attività istituzionale che comprende:

1. **Assistenza Ospedaliera**

Assistenza ospedaliera in regime di ricovero (ordinario e Day Hospital), ambulatoriale e consultoriale nei confronti dei pazienti, assistiti dal SSN o Solventi, affetti da patologia del sistema nervoso centrale e periferico (principalmente *sclerosi multipla, epilessia, morbo di Parkinson e altri disturbi del movimento, malattie neuromuscolari, tumori cerebrali, cefalee ed emicrania, paralisi cerebrali*

infantili, morbo di Alzheimer, malattie genetiche e metaboliche), erogata direttamente dalle U.O. di seguito indicate (vedi Piano di Organizzazione Aziendale) e successive attuazioni:

Neurochirurgia I	**Neurologia VI**
Neurochirurgia II	**Neurologia VII**
Neurochirurgia III	**Neurologia VIII**
Radioterapia	**Neurologia IX**
Neurologia I	**Neuropsichiatria Infantile**
Neurologia II	**Neurologia dello Sviluppo**
Neurologia III	**Neuroradiologia**
Neurologia IV	**Laboratorio di Patologia Clinica e Genetica Medica**
Neurologia V	**Neuroanestesia e Rianimazione**

2. **Attività di supporto o complemento all'attività clinica:**
    a) Archiviazione e riproduzione di documentazione clinica;
    b) Servizio farmaceutico ospedaliero;
    c) Servizio interno di recupero e rieducazione funzionale;
    d) Sperimentazione clinica di medicinali, modalità diagnostiche e terapeutiche e farmacovigilanza (Clinical Trial Center e Comitato Etico);

e) Erogazione a totale carico del Servizio sanitario nazionale, qualora non vi sia alternativa terapeutica valida, di medicinali inseriti in apposito elenco predisposto dalla Commissione Unica del Farmaco;

f) Attività medico-legale inerente all'accertamento dell'idoneità in ambito di diritto al lavoro (idoneità allo svolgimento di mansioni lavorative; controllo dello stato di malattia di dipendenti pubblici e privati);

g) Attività medico-legali in ambito necroscopico;

h) Gestione stato giuridico, economico e previdenziale del personale dipendente, dei borsisti e del personale non strutturato;

i) Attività amministrative correlate a quelle di diagnosi, cura e riabilitazione dei soggetti assistiti (gestione affari legali, stipula convenzioni, gestione protocollo, tenuta contabilità ed adempimenti conseguenti, acquisizione di beni e servizi, controllo apparecchiature, gestione manutenzioni ordinarie e straordinarie).

§ 3 Distribuzione dei compiti e delle Responsabilità nell'ambito delle strutture preposte al trattamento dei dati (19.2)

Sotto il profilo organizzativo, la Fondazione, ha modificato ed integrato la suddivisione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati, descritta nella comunicazione prot. 10382 del 22 Ottobre 2009, come di seguito riportato:

- **Il Titolare del trattamento**

Per tutti i trattamenti effettuati presso la Fondazione IRCCS Istituto Neurologico "Carlo Besta", il Titolare del trattamento dei dati, in conformità a quanto previsto dall'articolo 16 del nuovo testo dello Statuto della Fondazione approvato con Deliberazione del Consiglio di Amministrazione n. 140 del 21 Maggio 2009, è il Direttore Generale, a cui competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento, ha confermato ed aggiornato, con la nota sopra citata, le nomine di Responsabili del trattamento dei dati in capo ai Direttori delle U.O. di cui si compone la Fondazione ed ha affidato loro, per quanto di competenza, il compito di porre in essere ogni misura tesa a ridurre al minimo i rischi di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite con ogni mezzo ritenuto più idoneo.

- **I Responsabili**

Sono stati individuati quali responsabili del trattamento dei dati, i Direttori delle singole Unità Operative aziendali (sanitarie, scientifiche, amministrative e tecniche) in relazione ai trattamenti, informatizzati o manuali, che risultano direttamente gestiti dalle Unità Operative medesime.

I suddetti Direttori hanno il compito di garantire per quanto di propria competenza, e nell'area di propria pertinenza, l'attuazione ed il mantenimento delle procedure di sicurezza, stabilite dal Titolare, per la gestione delle informazioni su supporto cartaceo, ed in parte per la gestione delle informazioni mediante strumenti elettronici interfacciandosi, in quest'ultimo caso, con il Responsabile dei Sistemi Informativi.

Ai Responsabili del trattamento dei dati compete inoltre l'individuazione per iscritto, tra i propri sottoposti, degli Incaricati al trattamento dei dati e la vigilanza sulla corretta osservanza da parte degli Incaricati stessi, della disciplina sopraccitata e delle procedure impartite.

Per quanto concerne il personale medico si è invece ritenuto opportuno conferire al Direttore Sanitario il compito di incaricare tale personale per iscritto autorizzandolo al trattamento dei dati, in quanto i medici per poter espletare le proprie funzioni istituzionali (servizio di medico di guardia), hanno la necessità di poter accedere ai dati di tutti i pazienti ricoverati.

Analogamente, per il personale infermieristico, tecnico e di supporto, il compito di autorizzarli per iscritto al trattamento dei dati è stato affidato al Dirigente del SITRA, in quanto tale personale, per esigenze di natura organizzativa, può essere spostato da un reparto di degenza ad un altro.

- **Il Responsabile dei Sistemi Informativi**

E' stato individuato, nell'ambito dei Sistemi Informativi aziendali, il Responsabile della sicurezza informatica aziendale che ha il compito di coadiuvare il Titolare nel garantire l'ottemperanza, da parte dell'Azienda, agli adempimenti (misure minime) previsti dal Codice per i trattamenti effettuati con strumenti elettronici, definendo altresì le relative procedure comportamentali da adattare in Istituto per la sicurezza dei dati.

Inoltre, in ottemperanza al Provvedimento del Garante del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) l'Azienda, mediante l'ausilio del Responsabile sistemi informativi, ha provveduto a redigere l'elenco nominativo di tutti gli incaricati interni che svolgono funzione di amministratore di sistema (cfr. allegato 3 **elenco amministratori di sistema**) , quali:

- gestione e manutenzione di un sistema di elaborazione o di sue componenti;
- amministrazione di basi di dati;
- amministrazione di reti;
- amministrazione di apparati di sicurezza;
- amministrazione di software complessi.

In particolare, per i servizi di amministrazione di sistema che l'Azienda ha affidato in *outsourcing*, si è provveduto a richiedere, mediante lettera PROT. N.2057/09/ac del 27 febbraio 2009, alle ditte/società esterne la comunicazione degli estremi identificativi delle persone fisiche preposte a detta funzione. Tali dati sono stati integrati nel documento di cui sopra.

- **Gli Incaricati**

Sono tutti coloro che prestano servizio come dipendenti, collaboratori, borsisti, tirocinanti etc. presso la Fondazione. Sono nominati per iscritto dal Responsabile o direttamente dal Titolare e a loro è consentito in via esclusiva l'accesso ai dati personali, ed agli archivi permanenti, cui sono custoditi i dati, limitatamente ai trattamenti di propria competenza.

L'assetto organizzativo sopra descritto è integrato dai ruoli e dalle figure che la Fondazione ha individuato e nominato, a seguito di quanto richiesto dalla Regione Lombarda nell'ambito del progetto CRS-SISS, come indicato **nell'allegato I** al presente Documento , dal titolo *"Progetto CRS-SISS. Trattamenti di titolarità della Fondazione; misure di sicurezza adottate dalla stessa in conformità ai requisiti di legge ed ai requisiti della Regione Lombardia; "contributo"dei Responsabili designati"*.

4 Analisi dei rischi che incombono sui dati (19.3)

La Fondazione ha predisposto un'analisi rischi relativa ai trattamenti effettuati con strumenti elettronici improntata alla metodologia del Risk Management. Tale metodo prevede le seguenti fasi:

- **Individuazione dei rischi**

Consiste in una fotografia della situazione volta ad individuare le aree soggette a rischi e la tipologia dei rischi. Per ogni tipo di processo aziendale è stata individuata la tipologia dei dati trattati, gli applicativi che li contengono ed, in relazione a ciò, si è provveduto a valutare la conformità alle disposizioni di cui all'art. 34 ed al Disciplinare Tecnico (allegato B al codice privacy).

- **Valutazione dei rischi**

Il rischio relativo al pericolo individuato è valutato in termini di probabilità concrete che esso si verifichi e in funzione dell' entità del danno teorico per la Fondazione. Gli elementi essenziali che incidono sulla *probabilità* sono tre: le procedure, le tecnologie e le risorse umane.

Il rischio è dato dalla formula **R = P x D** dove R rappresenta la magnitudo del rischio, P configura la probabilità del verificarsi delle conseguenze e D evidenzia la gravità del danno.

Per valutare probabilità e gravità del danno si farà riferimento ai seguenti parametri:

Scala delle probabilità (P)

VALORE	LIVELLO
1	Improbabile
2	poco probabile
3	Probabile

Scala della gravità del danno (D)

VALORE	LIVELLO
1	lieve
2	medio
3	grave

Per quanto riguarda la numerica del rischio saranno applicati i seguenti valori:

R = 1 Rischio molto basso

R = 2 3 Rischio basso

R = 4 Rischio medio

R = 6 8 Rischio elevato

R = >8 Rischio molto elevato

- **Gestione dei rischi**

Propone delle raccomandazioni sulla base della differenza riscontrata tra la situazione di fatto e quella ottimale, con soluzioni tecniche e procedurali che hanno un impatto sulle risorse umane al fine di ridurre le probabilità che si verifichi il danno.

(cfr. allegato 2: Analisi dei Rischi relativa alla sicurezza informatica aziendale)

§ 5 Misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità (19. 4)

La Fondazione adotta, nell'ambito delle regole generali sopra descritte, un complesso di misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza volte ad assicurare un livello minimo di protezione dei dati personali.

- **Trattamenti con strumenti elettronici**

Accesso alla sala server

La maggior parte dei server aziendali si trova presso il nuovo locale tecnologico, in funzione dall'agosto 2010, ubicato al primo piano interrato della Fondazione IRCCS Istituto Neurologico "Carlo Besta". Gli ulteriori server si trovano nella sala CED sita al piano terra. L'accesso alle sale è consentito solo al personale abilitato, il quale vi accede previa autorizzazione del Responsabile e registrazione in portineria. I locali vengono tenuti chiusi e le chiavi sono custodite presso la portineria stessa. Qualora vi fosse la necessità di accedere ai locali Tecnici, da parte del personale del Servizio Informatico o del Servizio Tecnico, viene richiesta la chiave alla Portineria che provvede ad annotare ingresso e uscita sull'apposito registro.

Il locale è dotato di dispositivi antincendio, gruppo di continuità dell'alimentazione elettrica e impianto di condizionamento d'aria.

Per tutte le banche dati presenti presso la Fondazione, è in atto un Piano di Server Consolidation tendente a concentrare tutti i sistemi presso il nuovo locale tecnologico.

Il Piano favorirà anche la razionalizzazione e la standardizzazione delle misure minime di sicurezza da adottare in materia di Privacy.

Procedure di gestione delle credenziali di autenticazione

La Fondazione, con l'aiuto dei sistemi informativi, ha adottato, per disciplinare l'accesso agli strumenti elettronici e/o agli applicativi che contengono dati personali e sensibili, meccanismi di autenticazione informatica.

Per consentire agli incaricati del trattamento, di accedere agli strumenti e/o applicativi aziendali contenenti dati personali, sensibili e/o giudiziari, si è provveduto al rilascio di credenziali di autenticazione composte da codici identificativi personali (User ID), associati ad una parola chiave.

Salvo alcune limitate ipotesi relative ad elaboratori non in rete ovvero a sistemi operativi che consentono un unico livello d'accesso, non sono ammessi nomi identificativi di gruppo. Il codice identificativo assegnato ad un Incaricato del trattamento viene disabilitato se lo stesso ha dato le dimissioni, ha perso, per qualunque altro motivo, la qualità che gli consente di accedere ai dati ovvero non ha utilizzato tale codice per un periodo superiore ai sei mesi.

La Fondazione ha altresì definito le modalità di assegnazione delle password: le stesse saranno almeno di otto caratteri alfanumerici. Ogni utente Incaricato del trattamento dopo l'assegnazione iniziale modifica al primo accesso (logon) la propria password e comunque almeno ogni sei mesi e, laddove il trattamento ha ad oggetto dati sensibili, almeno ogni tre mesi.

Password e credenziali vengono attribuite, previa richiesta email da parte del Responsabile dell'UO o del Servizio di assegnazione del neoassunto, e inviate al nuovo utente attraverso posta elettronica. Insieme alle credenziali d'autenticazione vengono definiti i cosiddetti "privilegi d'accesso". Per ogni banca dati, i privilegi assegnati sono scelti tra i seguenti:

- Inserimento/Variazione di dati
- Lettura e stampa di dati
- Validazione di dati
- Cancellazione di dati

Per tutti gli applicativi aziendali che rientrano nell'area d'interesse del progetto CRS-SISS, l'autenticazione degli incaricati avviene mediante smart card, con tutte le procedure di sicurezza dettate e gestite dalla Regione Lombardia quale Titolare del trattamento.

Criteri e procedure per garantire la sicurezza delle trasmissioni dei dati

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il Titolare del trattamento dei dati ha stabilito, con il supporto tecnico dei sistemi informativi, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato.

I criteri sono definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In proposito si rinvia all'allegato 2 Analisi rischi relativi alla sicurezza informatica.

Protezione da accessi abusivi

In generale la protezione da accessi abusivi e dai potenziali danni ad essi legati avviene mediante l'impiego di "Firewalls" ed un sistema di "Content Filtering" (analisi del traffico sulla rete aziendale), di recente implementazione.

Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

L'ambito di trattamento consentito agli Incaricati verrà redatto ed aggiornato per categorie d'utenti nell'ambito di ciascuna unità organizzativa.

Custodia e conservazione dei supporti utilizzati per il back-up dei dati

I Sistemi Informativi, ovvero il Responsabile dell'Unità Operativa per i server ivi dislocati, sono responsabili della custodia e della conservazione di supporti utilizzati per il back-up dei dati.

Il luogo di conservazione dei supporti di back up è individuato in modo che gli stessi siano protetti da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni ed atti vandalici
- Incendio
- Allagamento
- Furto

Inoltre una copia dei dati importanti è archiviata in locali diversi e lontani da quelli dove sono stati eseguiti i back up.

L'accesso ai supporti utilizzati per il back-up dei dati è limitato per ogni banca di dati al:

· Responsabile del trattamento della sicurezza dei dati

· Incaricati del trattamento di competenza

· Sistemi Informativi

Altri supporti (utilizzo e smaltimento)

Per quanto concerne in generale i supporti di memorizzazione anche rimovibili (es. floppy disk, dischi ZIP, CD, etc.) contenenti dati personali, sensibili e giudiziari, la Fondazione ha prescritto agli incaricati di custodirli ed utilizzarli in modo da impedire accessi non autorizzati e trattamenti non consentiti.

In caso di necessità di riutilizzo o smaltimento dei supporti utilizzati per il trattamento dei dati, l'ufficio Sistemi Informativi Aziendali provvede all'eliminazione definitiva dei dati in essi contenuti tramite formattazione a basso livello o distruzione dei supporti stessi.

Istruzioni scritte per gli incaricati

La Fondazione, ha aggiornato e diffuso a tutti gli incaricati il regolamento contente le istruzioni per il corretto utilizzo degli strumenti informatici aziendali:

- Personal Computer
- Posta Elettronica
- Internet

Ciascun incaricato è stato istruito altresì su:

- segretezza e modalità di costruzione della parola chiave
- custodia dei dispositivi attribuiti a titolo di possesso ed uso esclusivo dell'incaricato (es. smart card);
- obbligo di non lasciare incustodito o accessibile lo strumento elettronico.

La Fondazione realizza anche eventi formativi rivolti a tutto il personale coinvolto nel trattamento dati mediante le postazioni di lavoro connesse con il SISS.

Gli argomenti riguardano:

1. La modalità di accesso al SISS:
2. Le regole di gestione delle informazioni (visualizzazione e registrazione):
3. Le attività che il personale deve effettuare per garantire al meglio la sicurezza della circolazione delle informazioni.

Per i dettagli si rinvia all'allegato 2 Analisi rischi relativi alla sicurezza informatica.

- **Trattamenti senza strumenti elettronici**

Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Nell'ambito di ciascuna Unità Operativa, i Responsabili garantiscono che l'accesso ai locali in cui vengono trattati dati personali, sensibili e/o giudiziari sia consentito esclusivamente al personale Incaricato del trattamento dei dati.

Il Responsabile ha cura di scegliere i locali e/o gli uffici in cui vengono svolte le operazioni di trattamento aventi ad oggetto i dati di cui sopra, nonché gli archivi destinati alla loro conservazione. La Fondazione vigila sulla corretta applicazione delle misure minime da parte dei Responsabili del trattamento dati avvalendosi anche dell'aiuto di soggetti esterni (i relativi rapporti sono conservati presso l'U.O. Affari Istituzionali).

Attualmente presso la Fondazione è presente:

- un'archiviazione temporanea di dati personali e sensibili a cura dei reparti di degenza e dai Laboratori della struttura, durante la quale la documentazione è conservata solitamente presso locali ad accesso selezionato qual i locali infermieristici, gli studi medici, i laboratori e/o le segreterie dei vari servizi. Ad essi accedono esclusivamente gli Incaricati del trattamento. Durante l'orario di lavoro sono generalmente presidiati dagli incaricati stessi e chiusi a chiave al termine della giornata lavorativa.
- un'archiviazione "storica" effettuata, parte in sede e parte affidata in outsourcing. Presso la sede della Fondazione la documentazione sanitaria è custodita presso l'archivio cartelle cliniche, la documentazione amministrativa è ubicata in archivio al piano interrato presso la sede di via Clericetti. Entrambi hanno un accesso selezionato e controllato mediante rilascio di singole autorizzazioni all'accesso e mediante registrazione in portineria dei soggetti autorizzati ad accedervi dopo l'orario di chiusura degli stessi.

In entrambi i locali inoltre è presente un sistema di rilevazione fumi e spegnimento incendio.

L'incarico di gestione archivio sanitario e custodia delle cartelle cliniche è affidato in outsourcing:

- alla società Italarchivi S.p.a. per le cartelle dei pazienti dimessi fino 31/08/2009.

- alla società Themis S.p.a. per le cartelle dei pazienti dimessi dal 1/09/2009. La Themis S.p.a. gestisce e custodisce le cartelle dopo averle scansite; le cartelle di pazienti dimessi prima del 1/09/2009 che effettuano nuovo ricovero presso la Fondazione vengono riconsegnate da Italarchivi e in seguito scannerizzate e custodite da Themis.

Per la definizione delle specifiche modalità di gestione si rimanda al vigente contratto in essere.

Ad integrazione delle misure di cui sopra, per la categoria dei dati genetici, la Fondazione IRCCS Istituto Neurologico con deliberazione n. 278 del 31 Agosto 2008 ha adottato una disciplina con cui individua particolari cautele tecniche ed organizzative al fine di assicurare che il suddetto trattamento, stante la natura dei dati raccolti, avvenga nell'assoluto rispetto dell'Autorizzazione del 22 febbraio 2007 emanata dall'Autorità Garante sulla privacy. La stessa disciplina è stata distribuita a tutti i Servizi e Laboratori interessati.

Misure di sicurezza contro il rischio di trattamento non consentito

L'ambito di trattamento consentito agli Incaricati è stato redatto ed aggiornato per categorie d'utenti nell'ambito di ciascuna unità organizzativa.

Istruzioni scritte per gli incaricati

La Fondazione, ha provveduto ad inviare a ciascuna Unità Operativa delle linee guida in materia di trattamento dei dati personali che forniscono agli incaricati una formazione relativa:

- ai rischi che incombono sui dati
- alle misure di sicurezza da adottare a protezione dei dati stessi
- alle responsabilità connesse al trattamento

- **Trattamenti con strumenti particolari : Videosorveglianza ai fini di sicurezza interna**

Presso la Fondazione è attivo un sistema di videosorveglianza che permette, la ripresa e la registrazione di immagini, a fini di sicurezza, di tutela del patrimonio e di controllo di determinate aree.

I dati acquisiti (memorizzati su un server dedicato) vengono trattati e conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali gli stessi sono stati raccolti e/ o successivamente trattati (max 96 ore). Il sistema provvede alla cancellazione automatica degli stessi trascorso il termine fissato per la conservazione.

La Fondazione ha provveduto a nominare il Responsabile dell'impianto ed i soggetti incaricati ad accedere alle immagini, nel rispetto delle vigenti disposizioni in materia di protezione dei dati personali e con l'adozione delle misure minime di sicurezza.

I dati eventualmente raccolti possono essere comunicati e/o diffusi solo su richieste effettuate, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento, o repressione dei reati.

Conformemente a quanto disposto dal provvedimento sulla videosorveglianza del 29 aprile 2004 è stato redatto il documento giustificativo delle scelte (approvato con Deliberazione n. 550 del 17 Dicembre 2008) e si è provveduto ad esporre in prossimità delle telecamere l'informativa di cui all'art. 13, integrata poi con degli avvisi sintetici, in conformità al modello fornito dall'Autorità Garante nel medesimo provvedimento.

- **Trattamenti con strumenti particolari : Videosorveglianza per monitoraggio pazienti**

La Fondazione IRCCS Istituto Neurologico ha adottato (con Deliberazione n. 550 del 17 Dicembre 2008) una regolamento per disciplinare il corretto utilizzo dei sistemi di videosorveglianza finalizzati al monitoraggio dei pazienti critici e non autosufficienti. Tale disciplina ha lo scopo di assicurare che il suddetto trattamento, stante la natura sensibile dei dati raccolti, avvenga nell'assoluto rispetto della riservatezza dei pazienti, ai sensi del D.lgs. 196/03 "Codice in materia di protezione dei dati personali".

§ 6 Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento degli stessi o degli strumenti elettronici (19.5)

Criteri e procedure per garantire l'integrità dei dati

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, la Fondazione, con il supporto tecnico dei Sistemi Informativi, effettua, per tutti i principali applicativi aziendali, un back up giornaliero.

I criteri sono definiti dai Sistemi Informativi stessi, in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni banca di dati sono definite le seguenti specifiche:

- I supporti utilizzati per le copie di back-up
- Il numero di copie di back-up effettuate
- Le procedure automatizzate e/o programmate utilizzate
- Le istruzioni e i comandi necessari per effettuare le copie di back-up, quando non sono eseguiti centralmente dai sistemi informativi.

Protezione da virus informatici

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita a causa di virus informatici, il Titolare si è dotato di idonei strumenti elettronici e di programmi che vengono aggiornati in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Riguardo la periodicità, i criteri sono definiti dall'Amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Al fine di prevenire le infezioni virali attualmente si sono adottate le seguenti misure:

1. ogni client aziendale è stato dotato di software antivirus.
2. tutti i server, sono dotati di software antivirus.

La frequenza degli aggiornamenti è automatica ed almeno giornaliera.

Ripristino della disponibilità dei dati

Per garantire la continuità dei servizi il Titolare dispone di hard disk multipli che garantiscono la disponibilità e l'integrità dei dati anche nel caso di guasto hardware di uno dei dischi che compongono il sistema.

Inoltre sui sistemi aziendali più critici sono stati previsti particolari accorgimenti come l'utilizzo di hardware e software ridondati con soluzioni clustering o il raddoppio di alcune parti critiche (esempio doppia scheda di rete, doppio alimentatore sui server).

Per fronteggiare eventi accidentali quali sabotaggi, disastri naturali etc.. sono previsti investimenti in piani di continuità operativa (piano di disaster recovery) che consentano il ripristino dei servizi informatici entro sette giorni minimizzando le conseguenze dell'interruzione dell'attività.

§ 7 Formazione degli incaricati (19.6)

La formazione degli incaricati avviene attraverso differenti modalità:

- **Al momento dell'ingresso in servizio**

La Fondazione, ha provveduto ad inviare, a ciascuna Unità Operativa, delle *linee guida (estese e sintetiche) in materia di trattamento dei dati personali* con l'obiettivo di fornire a tutti i dipendenti ed a tutti coloro che iniziano un rapporto di lavoro dipendente e/o di collaborazione con la Fondazione una formazione relativa:

- **ai rischi che incombono sui dati;**
- **alle misure minime di sicurezza da adottarsi per prevenire eventi dannosi;**
- **alla disciplina in materia di protezione dei dati personali;**
- **alle responsabilità connesse al trattamento dei dati.**
-

Le linee guida aziendali, saranno aggiornate ogni qualvolta sia necessario anche alla luce di eventuali cambiamenti organizzativi e tecnologici.

➢ **Aggiornamenti periodici della formazione**

E' stata affidata all'Ufficio Qualità e Risk Management, in collaborazione con l'UO Affari Istituzionali, un'attività di monitoraggio finalizzato alla verifica della corretta applicazione delle misure minime di sicurezza previste dalla normativa in materia di protezione dei dati personali, che prevede anche la formazione periodica dei Responsabili e degli Incaricati del trattamento dei dati.

Per l'anno 2011, in collaborazione con l'ufficio Formazione della Fondazione, saranno realizzati incontri formativi e momenti di condivisione singoli o di gruppo con l'obiettivo di informare e aggiornare il personale medico su questa tematica. Il contenuto del corso sarà presto definito nel dettaglio.

§ 8 Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamento di dati personali affidati in conformità al codice, all'esterno della struttura del Titolare (19.7).

La Fondazione in qualità di Titolare del trattamento, con riferimento a specifiche necessità aziendali, affida il trattamento dei dati in tutto o in parte, all'esterno della propria struttura provvedendo contestualmente alla nomina di tali soggetti esterni quali Responsabili del trattamento dei dati.

La nomina può avvenire con una lettera formale conservata a cura del Titolare del trattamento e controfirmata dal Responsabile per accettazione, ovvero essere inserita all'interno delle condizioni generali di un contratto o nell'ambito di una convenzione.

In entrambi i casi, contestualmente al conferire dell'incarico, vengono definiti compiti affidati ai Responsabili esterni, in relazione a quanto disposto dalle normative in vigore.

L'accettazione dell'incarico comporta per tali soggetti, l'onere di trattare e conservare i dati nel rispetto di quanto previsto dalla disciplina in materia di protezione dei dati personali ed in particolare l'onere di adottare, per la parte di trattamento che a loro compete, le misure minime di sicurezza previste dagli artt. 34 e 35 del codice e dal Disciplinare Tecnico allegato al codice privacy.

I Responsabili del trattamento dei dati così individuati, per le operazioni di trattamento loro affidate, hanno la legittimazione passiva in caso di violazione delle disposizioni di legge.

Qualora nello svolgimento dell'incarico i Responsabili esterni si avvalgano dell'operato di proprio personale interno o di altri soggetti esterni, hanno l'onere di nominarli Incaricati del trattamento dei dati e di provvedere alla loro formazione.

La Fondazione dal canto suo, deve assicurarsi che siano rispettate norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno, pertanto, nell'ambito dei suoi poteri di vigilanza e controllo, si riserva il diritto di procedere a verifiche periodiche sulle modalità di trattamento dei dati e sulle caratteristiche degli archivi cartacei ed informatici di tali soggetti esterni. Si riserva altresì la facoltà di richiedere a tali Responsabili del trattamento, di relazionare sulle misure di sicurezza adottate per il trattamento dei dati conformemente a quanto disposto dal D. Lgs. n.196 del 30 giugno 2003.

§ 9 Individuazione dei criteri da adottare per la cifratura o per la separazione dei dati inerenti lo stato di salute dagli altri dati personali dell'interessato (19.8)

I criteri individuati per garantire il rispetto della disposizione di cui al punto 19.8 del Disciplinare tecnico, si basano prevalentemente sulla separazione di tali dati dagli altri dati personali. Tale scelta è stata fatta in relazione alle competenze tecniche disponibili, alla necessità di effettuare un adeguamento delle procedure presenti ed ai costi previsti.

Al fine di consentire l'adempimento di tale misura è necessaria una forte revisione dell'architettura interna da farsi anche di concerto con i fornitori dei singoli applicativi. La strategia della Fondazione prevede che gli applicativi di futura acquisizione e/o quelli esistenti, oggetto di aggiornamento, siano implementate principalmente con tali meccanismi di separazione. Per questo la Fondazione con il supporto dell'Ufficio Sistemi Informativi, ha provveduto a richiedere ai fornitori degli applicativi contenenti dati personali/sensibili, concessi in licenza d'uso alla Fondazione una certificazione in merito al loro adeguamento con la normativa vigente in materia di protezione dei dati personali.

Ove le caratteristiche tecnologiche di alcuni prodotti, non fossero pienamente soddisfacenti i fornitori in questione dovranno comunicare, in tempi brevi, il piano degli interventi previsti per il relativo aggiornamento.

§ 10 Contributo relativo al progetto CRS-SISS.

Nell'aggiornare il Documento Programmatico Sulla Sicurezza dei dati la Fondazione ha redatto un contributo relativo al progetto CRS-SISS (allegato 1) dal titolo *Progetto CRS-SISS. Trattamenti di titolarità della Fondazione; misure di sicurezza adottate dalla stessa in conformità ai requisiti di legge ed ai requisiti della Regione Lombardia; "contributo"dei Responsabili designati* avente la funzione di illustrare le misure di sicurezza specifiche per l'attuazione del relativo progetto .

Il contributo è costituito da tre sezioni:

- **Sezione I: Trattamenti di titolarità della Fondazione effettuati per finalità amministrative e per finalità di cura.**
- **Sezione II: Misure di sicurezza adottate in conformità ai requisiti di legge ed ai requisiti della Regione Lombardia.**
- **Sezione III: Contributi delle Aziende Informatiche nominate Responsabili del trattamento nell'ambito di tale progetto.**

§ 11 Revisione e firma del documento

Il presente documento viene firmato, in calce, dal Direttore Generale della Fondazione IRCCS Istituto Neurologico "Carlo Besta", in qualità di titolare del trattamento dei dati e sarà oggetto di revisione o integrazione entro il 31 Marzo 2012.

Ad esso si allega, quale parte integrante del medesimo:

- il contributo relativo al progetto CRS-SISS (*allegato 1 Progetto CRS-SISS. Trattamenti di titolarità della Fondazione; misure di sicurezza adottate dalla stessa in conformità ai requisiti di legge ed ai requisiti della Regione Lombardia; "contributo"dei Responsabili designati*)
- l'analisi dei rischi relativi alla sicurezza informatica aziendale *(allegato 2).*
- l'elenco delle figure interne ed esterne che svolgono funzioni di amministrazione di sistema *(allegato 3 Elenco amministratori di sistema).*

Il DPS viene custodito presso la sede della Fondazione per essere esibito in caso di controlli e verrà reso noto ai Responsabili del trattamento dati mediante pubblicazione sulla intranet aziendale.

Milano, 30 marzo 2011

Il Direttore Generale

Dr. Giuseppe De Leo

ALLEGATO I

Progetto CRS-SISS. Trattamenti di titolarità della Fondazione; misure di sicurezza adottate dalla stessa in conformità ai requisiti di legge ed ai requisiti della Regione Lombardia; "contributo" dei Responsabili designati

Introduzione

La Fondazione I.R.C.C.S. Istituto Neurologico "Carlo Besta", redige il presente contributo in qualità di Titolare dei trattamenti effettuati per finalità amministrative e di cura relativi al progetto CRS – SISS.

Il contributo costituisce parte integrante del DPS adottato dalla Fondazione (capitolo "Interconnessione con il Crs-Siss") e ha la funzione di illustrare le misure di sicurezza specifiche per l'attuazione del Progetto Crs – Siss come di seguito sintetizzate:

SEZIONE I
TRATTAMENTI DI TITOLARITÀ DELLA FONDAZIONE EFFETTUATI PER FINALITÀ AMMINISTRATIVE E PER FINALITÀ DI CURA.

1. TRATTAMENTI INTERESSATI

La tipologia di trattamenti (per finalità amministrative e cura) rispetto ai quali l'Azienda risulta essere Titolare:

L'Azienda è Titolare relativamente ai trattamenti amministrativi di:

- **Registrazione, Organizzazione, Conservazione, Consultazione, Elaborazione, Selezione, Estrazione, Interconnessione, Raffronto, Utilizzo e Comunicazione** relativi a prescrizioni, prenotazioni, erogazioni, eventi sanitari, flussi di rendicontazione e anagrafica.

L'A.O. relativamente ai trattamenti per finalità di cura è Titolare dei trattamenti di:

- **registrazione, conservazione, elaborazione, selezione, estrazione, interconnessione, raffronto e comunicazione** relativa alla gestione delle basi dati inerenti l'utilizzo del Fascicolo Sanitario Elettronico (FSE) e del consenso.

1.2 Infrastruttura di sicurezza

1.2.1. Responsabilità e Organizzazione di sicurezza

RUOLO	RESPONSABILITA'
Responsabile dei Servizi Direttore Generale Dr. Giuseppe De Leo	*Coordina le attività della propria organizzazione e la impegna formalmente verso il CRS-SISS. E' il responsabile gerarchico della azienda che aderisce al progetto.*
Manager della sicurezza Responsabile Sistema Informatico Ing. Andrea Migliaro e Responsabile Flussi Dr. Alberto Maspero	*Responsabile del management della sicurezza per la propria organizzazione, elabora, aggiorna e pubblica la politica di sicurezza dei sistemi informativi, per quanto di competenza. Coordina la redazione delle Istruzioni Operative. Sovrintende alla corretta e puntuale applicazione della Policy definita per quanto di loro pertinenza.* *Particolare riguardo, per quanto attiene la figura del Responsabile Sistema Informatico, alle misure da adottare per la sicurezza dei servizi nell'ambito del CRS-SISS.*
Data Protection Manager Responsabile flussi sanitari informatici Sig. Rocco Zagari	*Definisce appropriate misure per la conservazione ed il trattamento dei dati personali nella propria organizzazione e verifica l'applicazione di tali misure per il corretto adempimento delle norme sul trattamento dei dati personali.*
Amministratore dei Sistemi e dell'Infrastruttura di Rete Ing. Andrea Migliaro	*È responsabile dell'amministrazione del software, hardware e infrastruttura di rete. Effettua monitoraggio ed auditing delle misure tecniche di sicurezza.*
Referente IRT Dr.ssa Paloma Callori	*È il riferimento per l'IRT(Incident Response Team) del CRS-SISS e per tutte le comunicazioni con il personale inerenti la continuità o la sicurezza del servizio.*
Operatore / Addetto	*Personale* ***INCARICATO*** *del trattamento che eroga ed accede ai servizi del CRS-SISS*

1.2.2. Formazione INCARICATI interni alla A.O.

La Fondazione, per favorire l'attenzione al trattamento dei dati nel rispetto della legge sulla privacy, realizza eventi formativi rivolti a tutto il personale coinvolto con il trattamento dati relativi alle postazioni di lavoro connesse con il SISS.
A seguito di un'analisi dei bisogni, è stato realizzato un progetto di formazione in cui è prevista la presentazione della logica di funzionamento del SISS e delle attività che il personale deve effettuare per garantire al meglio la sicurezza del trattamento dei dati.

Gli argomenti relativi al "Trattamento dei dati" sono:

4. La modalità di accesso al SISS:
   - La SmartCard Operatore
   - Il codice PIN e PUK
   - Il codice PIN FIRMA
   - La firma digitale e la sua sicurezza

5. Le regole di gestione delle informazioni (visualizzazione e registrazione):
   - Il consenso al trattamento dei dati dell'assistito.
   - La gestione delle informazioni nel caso in cui l'assistito ha espresso il consenso al trattamento dei suoi dati nel SISS e nel caso in cui non esprime il consenso.
   - Le informazioni a cui un operatore della Socio Sanità può accedere in base al ruolo che occupa.

6. Le attività che il personale deve effettuare per garantire al meglio la sicurezza della circolazione delle informazioni:
   - Portare sempre con se la propria SmartCard Operatore
   - Non divulgare i codici PIN della propria SmartCard
   - La SmartCard è personale e non va condivisa con altri

- In caso di smarrimento della SmartCard o dei Codici PIN/PUK è necessario contattare gli Operatori PDA/PDR della Fondazione.

SEZIONE II
MISURE DI SICUREZZA ADOTTATE IN CONFORMITÀ AI REQUISITI DI LEGGE ED AI REQUISITI DELLA REGIONE LOMBARDIA.

2. IMPATTI DI SICUREZZA

2.1 IMPATTI ARCHITETTURALI

L'interconnessione del sistema informatico della Fondazione con il CRS-SISS, avviene tramite il PdL (Posto di Lavoro) o tramite il F.E. (Front End della porta Applicativa).
Mentre il F.E. è sempre configurato e gestito dal progetto senza intervento né di tipo applicativo né sistemistico da parte dell'azienda, il PdL sia in configurazione per supportare gli accessi di tipo Application to Application, che nella configurazione in cui interagisce con il CRS-SISS via Web Browser, dopo un'iniziale installazione e configurazione fatta dal progetto è gestito direttamente dalla Fondazione.

2.2 IMPATTI OPERATIVI

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

- la base dati centralizzata della Regione Lombardia (Dominio Centrale) è concepita per separare logicamente e anche fisicamente i dati anagrafici da quelli afferenti gli eventi sanitari di rilevanza amministrativa. In questo modo non è possibile ricavare informazioni sullo stato di salute di un assistito avendo accesso ad un solo insieme omogeneo di dati;

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

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

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

2.3 IMPATTI ORGANIZZATIVI

La Fondazione in qualità di Responsabile del Trattamento dei dati attinenti al progetto Siss, ha provveduto a nominare formalmente il proprio personale , Incaricato del trattamento che eroga ed accede ai servizi del Siss. Ogni operatore è ammesso esclusivamente all'accesso di un numero specifico di funzioni in base al proprio ruolo e alle proprie responsabilità. Il criterio di autorizzazione si applica a livello di programma, di funzione applicativa e di singolo elemento di dati di una transazione.

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

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

2.4 GESTIONE DEL RISCHIO

Si rinvia all'allegato "analisi dei rischi informatici" del DPS aziendale che affronta l'analisi e la gestione del rischio informatico della azienda in maniera complessiva.

2.5 SICUREZZA FISICA

Si rinvia allo specifico paragrafo del DPS aziendale ed all'allegato "analisi dei rischi informatici" al DPS aziendale che tratta le misure di sicurezza fisica già in vigore in azienda.

2.6 SUPPORTI DI MEMORIZZAZIONE

Si rinvia allo specifico paragrafo del DPS aziendale ed all'allegato "analisi dei rischi informatici" al DPS aziendale che tratta le regole in vigore nella azienda per la gestione, custodia, riutilizzo dei supporti di memorizzazione che contengono o hanno contenuto informazioni personali e informazioni personali sensibili.

2.7 SICUREZZA LOGICA

Si rinvia allo specifico paragrafo del DPS aziendale ed all'allegato "analisi dei rischi informatici" al DPS aziendale, che tratta delle misure e procedure di sicurezza logica valide per tutti gli apparati informatici che trattano dati personali e sensibili.

Inoltre riportiamo di seguito le procedure e le misure specifiche della interconnessione con il CRS-SISS, nonché la procedura di Gestione delle Carte a Microprocessore.
Ogni potenziale utente dei sistemi o delle banche dati è associato ad un identificativo (user-id). Prima che un Utente acceda al sistema, agli archivi informatici o alla rete, ne **"deve"** essere verificata l'identità mediante un successivo livello di controllo "autenticazione".

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

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

Dopo il riconoscimento autenticato dell'utente e prima di consentire allo stesso l'accesso ai dati, la validità della richiesta di accesso è verificata con un controllo basato su una politica di controllo accessi "chiusa", cioè nel senso che "tutto ciò che non è esplicitamente concesso è vietato".
Lo schema di autorizzazione per l'accesso alle risorse / servizi in uso **"è"** valutato, con riguardo alle necessità operative degli incaricati, ciascun incaricato **"è"** ammesso a trattare soltanto i dati che sono strettamente necessari alla sua funzione, tale schema **"deve"** essere riveduto regolarmente.
Le applicazioni e le infrastrutture inerenti l'erogazione dei servizi SISS applicano un criterio d'autorizzazione d'accesso basato su ruoli, che prevede un ambito di diffusione dei dati

strettamente necessario alle esigenze degli incaricati. Non **"è"** mai permesso l'accesso alle risorse (dati, servizi, sistemi) se non dopo una corretta identificazione ed autenticazione dell'incaricato.

Gestione Carte a Microprocessore

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

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

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

- Responsabilità dell'utilizzo e della custodia delle Carte a Microprocessore.
- Cura nella gestione confidenziale del Personal Identification Number (PIN) di accesso alla Carta.
- Maggiori difficoltà incontrate nella gestione delle Carte.

La Carta a Microprocessore riveste per l'Operatore della azienda sociosanitaria una doppia funzione:

- Permette all'Operatore di essere Identificato ed autenticato dal CRS-SISS in modalità Forte.
- Permette all'Operatore di firmare digitalmente i documenti informatici scambiati con il CRS-SISS.

La validità e la sicurezza di ciascuna delle due funzioni si basa, oltre che naturalmente sulla robustezza intrinseca degli algoritmi crittografici e sulla affidabilità e correttezza della Struttura (PKI) che rilascia e gestisce i certificati (Certification Authority), su due fondamentali requisiti a carico dell'Operatore della azienda sociosanitaria:

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

Inizializzazione

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

Utilizzo e Gestione

- I **PIN** d'accesso alle funzioni (autenticazione e firma), relative ad un Operatore Titolare di carta sono strettamente personali e non **devono** assolutamente essere comunicati ad altri.
- L'Operatore Titolare di carta **deve** evitare di trascrivere i **PIN** in chiaro, su carta o su altro supporto informatico.
- L'Operatore Titolare di carta, è espressamente invitato a modificare il **PIN** nei casi ne ritenga compromessa la confidenzialità.
- L'Operatore Titolare di carta **deve** archiviare in modo sicuro i due codici **PUK** (**PIN** Unblocking Key), con i quali gli è possibile sbloccare la Carta a Microprocessore dopo il ripetuto (7 volte) inserimento errato del PIN.

- La perdita della Carta a Microprocessore o la compromissione dei codici **PUK**, **deve** essere prontamente comunicata dall'Operatore Titolare alla Certification Authority (CA), secondo la procedura definita nel Manuale Operativo della CA per la richiesta di revoca dei certificati.
- L'Operatore Titolare di carta **deve** gestire con diligenza la Carta a Microprocessore assegnatagli, evitando le situazioni in cui ne perda il controllo (es. lasciare la Carta incustodita).
- L'Operatore Titolare di carta **deve** prontamente segnalare al proprio Manager della Sicurezza le violazioni di sicurezza relative alle Carte a Microprocessore. Tra le violazioni di sicurezza sono incluse quelle situazioni in cui all'Operatore Titolare di carta viene richiesto, specialmente se da parte di altri utenti del CRS-SISS, di comunicare i propri PIN di abilitazione.

Carta Non Intestata

Le regole di gestione sopra riportate, sono valide per tutte le tipologie di carte operatore (Carta Nominativa, Carta Intestata, Carta Non Intestata). Per la specifica tipologia della Carte Non Intestate si riportano ulteriori considerazioni di sicurezza come dedotte dal documento (rif [3]).

Caratteristiche della Carta Non Intestata

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

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

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

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

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

- Farmacista Collaboratore;
- Amministrativo di Azienda;
- Impiegato ASL di Scelta/Revoca;
- Ufficio Privacy;
- Infermiere;
- Altro Operatore di Emergenza;
- Operatore di Call-center;
- Impiegato del Punto di Adesione/ Punto di Registrazione (PdA/PdR).

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

In questi casi, la struttura può preventivamente richiedere carte non intestate pur non conoscendo i nominativi delle persone alle quali dovranno essere assegnate. Queste carte verranno poi attivate nel momento in cui sarà noto l'operatore al quale assegnarle, minimizzando così i tempi necessari per rendere operativo nel CRS-SISS il nuovo operatore grazie all'anticipazione del processo di produzione.

Le carte non intestate che vengono richieste verranno consegnate al PdA/PdR di riferimento del richiedente (e.g. PdA/PdR della ASL per i MMG, PdA/PdR dell'Azienda per le AO). Nel momento in cui un operatore dovrà essere dotato di una carta non intestata, dovrà recarsi presso il PdA/PdR.

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

Solo nel momento in cui una carta "non ad personam" (ovvero non intestata) viene assegnata ad un operatore viene generata la relativa quantità di sicurezza (i.e. codici PIN/PUK, ecc.).
Quando l'operatore non dovrà più utilizzare il CRS-SISS presso la struttura che l'aveva dotato di carta non intestata, dovrà restituire la carta alla PdA/PdR di riferimento.

2.8 LOG DEI DATI

La raccolta, la diffusione ed il salvataggio/ripristino dei log riguardanti le attività relative alla fruizione/erogazioni dei servizi CRS-SISS, seguono le stesse regole in vigore nella organizzazione aziendale per la gestione dei log relativi ai servizi che trattano dati personali e sensibili. I log sono conservati per 24 mesi e le informazioni raccolte permettono di risalire al momento, all'identità dell'Utente dove significativa, ed all'attività svolta

2.9 PROTEZIONE DATI SANITARI

I programmi realizzati dal progetto CRS-SISS:

- sono installati e configurati da LISIT (porta applicativa) e da accreditati Provider di servizi (posto di lavoro);
- vengono periodicamente monitorati dal Centro Gestione Integrata (CGI) del progetto;

garantiscono che:

- i dati sanitari **"sono"** trasmessi in rete protetti da adeguati algoritmi di cifra;
- I dati sanitari quando presenti negli archivi informatici **"sono"** memorizzati cifrati o disaggregati dai dati personali in modo che la loro compromissione non permetta di ricondurre il dato sanitario alla specifica persona.

2.10 PROGRAMMI PERICOLOSI

Tutti gli apparati informatici utilizzati dalla Fondazione per trattare dati personali, sono protetti contro l'azione di programmi pericolosi. Eccezione formale, ma non sostanziale, a questa regola riguarda gli apparati di F.E. (della Porta Applicativa) di interconnessione al CRS-SISS. Per questi apparati l'azienda sociosanitaria non applica direttamente nessuna protezione, ma richiede al gestore del CGI (Lombardia Informatica SPA con i suoi Partner) che gestisce direttamente questi apparati, visibilità dell'impegno da questi preso per proteggere, conformemente alla legge, gli apparati sotto il suo controllo.

2.11 PROCEDURA DI BACKUP/CONTINUITÀ DEL SERVIZIO

Per garantire l'integrità dei dati trattati ed il ripristino del servizio a fronte di danneggiamento dei dati o degli strumenti informatici che li trattano, la Fondazione pianifica per tutti i trattamenti di cui è **TITOLARE** un'attività di "back-up" di tali dati, e dove necessario progetta architetture ad alta disponibilità dei sistemi su cui i dati risiedono.
Si fà riferimento direttamente allo specifico paragrafo del DPS, che descrive le regole in vigore nella organizzazione della Fondazione per la gestione dei back-up dei sistemi che trattano dati personali e sensibili.

2.12 SICUREZZA DELLA CONNETTIVITÀ AL CRS-SISS

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

- Prima di permettere l'accesso agli apparati, **verifica l'identità del personale inviato dal Provider**. A tal riguardo il Provider è tenuto ad informare preventivamente l'azienda sulla propria procedura di installazione/manutenzione evidenziando i momenti di controllo che l'azienda può esercitare.

- Durante l'attività svolta dal personale del Provider, **esercita una supervisione diretta sulle attività condotte dal personale del Provider**.
- Nel caso il personale del Provider debba accedere al sistema informativo senza restrizioni d'accesso, **si cautela preventivamente mediante rimozione o cifratura dei dati di privacy**.
- Al termine dell'installazione, l'amministratore dei sistemi dell'azienda **prende in carico gli apparati secondo le regole di gestione degli stessi, mediante la sottoscrizione del verbale di collaudo** che il personale del Provider rilascia firmato per attestare l'esito positivo dei controlli e delle attività di installazione e/o manutenzione eseguita.

Per la procedura aziendale si rinvia al paragrafo del Dps aziendale e del regolamento interno

2.13 CONTROLLI VERIFICHE E AUDIT

La Fondazione pianifica un'attività di auditing di prima parte (personale interno) con periodicità semestrale, sulla sicurezza del proprio sistema informatico comprendente gli apparati d'interconnessione al CRS-SISS, che tratta dati personali e sensibili.
L'audit sarà centrato oltre che sulla verifica della corretta ed efficace adozione delle misure minime di sicurezza adottate, anche sul livello di formazione degli ***INCARICATI*** nominati e sul rispetto delle istruzioni impartite.

SEZIONE III: CONTRIBUTI DELLE AZIENDE INFORMATICHE NOMINATE RESPONSABILI DEL TRATTAMENTO NELL'AMBITO DI TALE PROGETTO.

3. Contributi delle aziende informatiche nominate responsabili del trattamento

Le Aziende Informatiche, nominate Responsabili del trattamento dati da codesta Azienda Sanitaria nell'ambito del Progetto CRS-SISS, sono:

- Lombardia Informatica S.p.A.
- Lombardia Integrata S.p.A.
- Lutech S.p.A.
- Almaviva S.p.A.
- Santer Reply S.p.A.
- Transcom Worldwide S.p.A.

Anche per questo anno i contributi nei quali le suddette Aziende Informatiche hanno descritto come sono stati realizzati gli interventi operativi necessari per rispondere ai requisiti di sicurezza indicati da codesta Fondazione all'atto della loro designazione quali Responsabili, sono rintracciabili nell'area riservata del sito del progetto (www.crs.lombardia.it).

In particolare i contributi contengono un riferimento costituito da:

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

FONDAZIONE I.R.C.C.S.
ISTITUTO
NEUROLOGICO
CARLO
BESTA

Analisi dei Rischi Informatici 2011
FONDAZIONE I.R.C.C.S.
ISTITUTO NEUROLOGICO
"CARLO BESTA"

Fondazione I.R.C.C.S. Istituto Neurologico Carlo Besta
Via Celoria 11, 20133 Milano - Tel 02 2394 1 - CF 01668320151 - PI 04376340156 - www.istituto-besta.it

INDICE

INTRODUZIONE

L'analisi della situazione esistente relativa alle modalità di gestione dei dati personali e sensibili mediante strumenti elettronici, è stata improntata alla metodologia del Risk Management. La metodologia prevede i seguenti step:

Individuazione dei rischi

Consiste in una fotografia della situazione volta ad individuare le aree soggette a pericolo: ci si limita a descrivere il pericolo senza valutare né le misure preventive già attuate, né il rischio connesso a quel pericolo.

Valutazione dei rischi

Provvede a valutare il rischio relativo al pericolo individuato in termini di probabilità concrete ed entità del danno teorico. La valutazione dei rischi prende in considerazione trasversalmente tutti gli aspetti del sistema ICT (Applicativi, Server, Rete, Infrastruttura e Organizzazione), mantenendo come obbiettivo di analisi l'applicativo che tratta determinati dati.

SICUREZZA DEI TRATTAMENTI

Metodologia della valutazione dei rischi e delle responsabilità

Ogni trattamento di dati personali é soggetto a rischi imputabili, principalmente, a due fattori caratteristici delle tecnologie dell'informazione:

- ✓ L'***inaffidabilità***: non si ha la garanzia del continuo e corretto funzionamento delle componenti hardware e di quelle software;
- ✓ L'***esposizione alle intrusioni informatiche:*** la continua evoluzione delle reti e l'enorme diffusione del loro utilizzo rendono i sistemi informativi aziendali (nodi di rete) sempre più soggetti al rischio delle intrusioni non consentite e del danneggiamento o cancellazione dei dati contenuti nelle banche dati.

A ciò si deve aggiungere l'imponderabilità dell'errore umano nel corso del trattamento.

Un sistema informativo sicuro deve provvedere, innanzitutto, alla tutela di ciascun nodo e, successivamente, delle connessioni o network nel suo insieme. Un sistema informativo sicuro soddisfa, come norma generale, le seguenti proprietà:

- ✓ ***Disponibilità:*** l'informazione e i servizi che il sistema eroga devono essere a disposizione degli utenti del sistema stesso compatibilmente con i livelli di servizio e con gli incarichi di trattamento detenuti;
- ✓ ***Integrità:*** l'informazione e i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a compiere tali operazioni;
- ✓ ***Autenticità:*** la provenienza dei dati deve essere garantita e certificata;
- ✓ ***Confidenzialità (riservatezza):*** l'informazione gestita del Sistema Informativo può essere fruita solo dalle persone autorizzate a compiere tale operazione.

La metodologia adottata per la valutazione dei rischi prevede di seguire i seguenti step:

- ✓ ***Identificazione delle sorgenti di rischio*** che, manifestamente, espongono l'azienda ad un rischio potenziale;
- ✓ ***Distinzione delle sorgenti di rischio in :*** comportamenti degli operatori; eventi relativi agli strumenti; eventi relativi al contesto.
- ✓ ***Individuazione dei rischi*** esaminando le modalità operative di inserimento, archiviazione, trattamento e distruzione dei dati, le modalità di accesso alle aree e alle apparecchiature e la presenza di misure di sicurezza e/o di sistemi di prevenzione.

- ✓ ***Stima dei rischi d'esposizione*** ai fattori di pericolo riscontrati nell'ambiente di lavoro con una particolare valutazione dell'entità delle esposizioni summenzionate, della gravità degli effetti che ne possono derivare e della probabilità che tali effetti si manifestino.
- ✓ ***Programmazione degli interventi di protezione*** previsti, pianificando i tempi di realizzazione degli interventi tenendo conto della tecnologia conosciuta, degli standard d'esecuzione del lavoro e, ovviamente, dell'entità del rischio così come valutato secondo i criteri sopra esposti.

Criteri di valutazione del rischio

Ogni rischio, cui sono potenzialmente sottoposti i dati personali nella fase del loro trattamento, sono valutati e "dimensionati" affidando loro un ***indice di rischio (I.R.).*** L'indice di rischio si ottiene dalla combinazione di due fattori: ***l'indice di probabilità (I.P),*** definito come la possibilità che un evento accada, e ***l'indice di danno o gravità (I.D.),*** definito come la gravità del danno che l'evento accaduto ha causato.

- ***Indice di probabilità (I.P.):*** indica la probabilità che un evento dannoso accada, in funzione delle condizioni di sicurezza vigenti e dei dati statistici disponibili; può variare tra i valori **1** e **4** secondo la seguente classificazione:

Classificazione	I.P.	Anomalia rilevata
Improbabile	1	*Può provocare un danno per la concomitanza di più eventi poco probabili e indipendenti. Non si sono mai verificati episodi*
Possibile	2	*Può provocare un danno solo in condizioni sfortunate di eventi. Sono noti episodi sporadici*
Probabile	3	*Può provocare un danno anche se non in modo automatico o diretto. E' noto qualche episodio in cui alla mancanza ha fatto seguito il danno.*
Molto probabile	4	*Esiste una correlazione diretta tra mancanza rilevata e il verificarsi del danno. Si sono già verificati danni per la stessa mancanza nella stessa azienda o in aziende simili*

- ***Indice di danno (I.D.):*** indica la dimensione del danno che si potrebbe causare, in termini sia quantitativi che qualitativi. Anch'esso può variare tra i valori **1** e **4** secondo la seguente classificazione:

Classificazione	I.D.	Anomalia rilevata
Lieve	*1*	*Costi monetari e di immagine lievi*
Medio	*2*	*Costi monetari e di immagine di media entità*
Grave	*3*	*Costi monetari e di immagine elevati*
Gravissimo	*4*	*Costi monetari e di immagine di elevatissima entità*

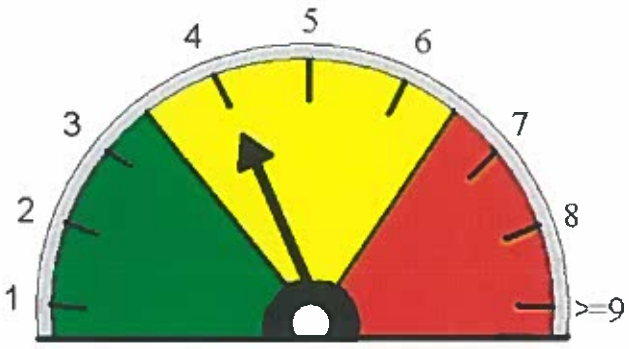
Sulla base dei due indici sopra descritti si può affermare che:

RISCHIO (I.R.)= PROBABILITA' (I.P.) X DANNO (I.D.)

INDICE DI RISCHIO=I.P. X I.D.

Secondo quanto espresso graficamente nel seguente schema, il rischio cui sono sottoposti i dati personali, sarà tanto maggiore quanto più elevati saranno gli indici ***I.P.*** e ***I.D.*** del loro trattamento.

R = 1	Rischio molto basso
R = 2 3	Rischio basso
R = 4 6	Rischio medio
R = 7 9	Rischio elevato
R = > 9	Rischio molto elevato



Non esistendo attualmente standard normativi o tecnici di riferimento, la valutazione del rischio per ogni trattamento dati è una valutazione soggettiva operata dai soggetti attivi del T.D.. L'utilizzo dell'indice di rischio (I.R.), pur non eliminando l'errore insito in tale valutazione, permette di stabilire delle priorità nell'applicazione delle procedure di prevenzione e protezione e di costruire valori numerici di rischiosità facilmente confrontabili. I Trattamenti che presentano un indice di rischio più elevato richiederanno, relativamente ad altri con indice di rischio meno elevato, un'attenzione particolare nell'adozione delle procedure di sicurezza (priorità nell'applicazione delle misure di protezione e prevenzione, tempi brevi nell'applicazione delle stesse).

PERICOLI INDIVIDUATI IN CONFORMITÀ AL D.LGS 196/2003

Tale analisi si basa su informazioni acquisite esclusivamente per via verbale e intende fornire un prospetto di massima per valutare quali possono essere i rischi legati all'uso di sistemi informatici.

Nella seguente sezione verrà fornita l'analisi della struttura informatica dell'Azienda, considerando essenzialmente la sicurezza logica ed in particolar modo le fattispecie e le misure indicate dagli articolo 34 della normativa e dall'Allegato B (Disciplinare Tecnico).

Tra gli altri aspetti ed aree di esame saranno quindi considerati i seguenti punti:

- **Autenticazione informatica (art. 34)**
- **Adozione di procedure per la creazione e gestione delle credenziali d'autenticazione (art. 34)**
- **Utilizzazione di un sistema di autorizzazione (art. 34)**
- **Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici (art. 34)**
- **Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici (art. 34)**
- **Adozione di procedure per la custodia delle copie di sicurezza (art. 34)**

CRUSCOTTO

Ambito Applicativo	Dati		Applicazioni			Server		Rete	Infrastruttura	Organizzazione	Probabilità	Rischio
	Sensibili	Valore	Valutazione sulla probabilità di perdita di disponibilità	Valutazione sulla probabilità di impersonificazione	Valutazione sulla probabilità di accesso illecito	Valutazione sulla probabilità di perdita di disponibilità	Valutazione sulla probabilità di accesso illecito	Valutazione sulla probabilità di inefficienza della rete	Valutazione sulla inegualezza dell' infrastruttura	Valutazione sulla inegualezza dell' organizzazione		R = D X P
		Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo		
Ambito Sanitario												
[illegible]	SI	3	2	1	1	1	1	2	2	2	3	
[illegible]	SI	3	2	1	1	1	1	2	2	2	2	
[illegible]	SI	3	2	1	1	1	1	2	2	2	1	
[illegible]	SI	3	2	1	1	1	1	2	2	2	1	
[illegible]	SI	3	1	1	1	1	1	2	2	2	1	
[illegible]	SI	3	1	1	1	1	1	2	2	2	1	
[illegible]	SI	3	2	1	1	1	1	2	2	2	2	
[illegible]	SI	3	2	1	1	1	1	2	2	2	2	
[illegible]	SI	3	2	2	2	1	1	2	2	2	1	
[illegible]	SI	3	1	1	1	1	1	2	2	2	2	
[illegible]	SI	3	1	1	1	1	1	2	2	2	2	
[illegible]	SI	3	1	1	1	1	1	2	2	2	2	
[illegible]	SI	3	1	1	1	1	1	2	2	2	2	
[illegible]	SI	3	2	2	2	1	1	2	2	2	1	

Ambito Applicativo	Dati		Applicazioni			Server		Rete	Infrastruttura	Organizzazione	Probabilità	Rischio
	Sensibili	Valore	Valutazione sulla probabilità di perdita di disponibilità	Valutazione sulla probabilità di impersonificazione	Valutazione sulla probabilità di accesso illecito	Valutazione sulla probabilità di perdita di disponibilità	Valutazione sulla probabilità di accesso illecito	Valutazione sulla probabilità di inefficienza della rete	Valutazione sulla inegualezza dell' infrastruttura	Valutazione sulla inegualezza dell' organizzazione		R = D X P
		Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo		
Ambito Amministrativo												
Applicativo Bilancio	NO	2	2	2	2	1	1	2	2	2	1	
Applicativo web Dikeinweb	NO	2	2	2	2	1	1	2	2	2	1	
Applicativo Gestione Personale (MEDLINE)	SI	3	2	2	2	1	1	2	2	2	1	
Applicativo Gestione Work Flow (INFOLINE)		3	2	2	2	1	1	2	2	2	1	
Applicativi controllo di gestione (PEGOS)	NO	2	2	2	2	1	1	2	2	2	2	
Applicativo web Gestione Apparecchiature Biomediche (ASSETPLUS)	NO	1	2	2	2	1	1	2	2	2	1	
Gestione Allarmi Temperature Frigoriferi (SPY-LOG)	NO	1	2	2	2	1	1	2	2	2	1	
BALANCE SCORE CARD web	NO	2	2	2	2	1	1	2	2	2	1	
Sistema Videosorveglianza Telecamere	NO	3	"	"	"	"	"	2	2	2	1	
Ambito della Comunicazione												
Posta elettronica web istituzionale (Microsoft Exchange - Outlook Web Address)	SI	2	2	1	1	1	1	2	2	2	2	
Ambito Gestione Informatizzata dei Documenti												
Applicativo web Gestione Delibere	NO	1	2	2	2	1	1	2	2	2	1	
Applicativo web Gestione Protocollo	NO	1	2	2	2	1	1	2	2	2	1	
Applicativo Gestione Rubrica Direzionale	NO	1	2	2	2	1	1	2	2	2	1	

	Dati		Applicazioni			Server		Rete	Infrastruttura	Organizzazione	Probabilità	Rischio
	Sensibili	Valore	Valutazione sulla probabilità di perdita di disponibilità	Valutazione sulla probabilità di impersonificazione	Valutazione sulla probabilità di accesso illecito	Valutazione sulla probabilità di perdita di disponibilità	Valutazione sulla probabilità di accesso illecito	Valutazione sulla probabilità di inefficienza della rete	Valutazione sulla inegualezza dell' infrastruttura	Valutazione sulla inegualezza dell' organizzazione		R = D X P
		Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo	Valori: 1= Basso 2= Medio 3= Alto 4= Altissimo		
Ambito Workstation												
Windows XP / 2000 / NT	NO	1	"	"	"	"	"	2	2	2	1	
Mac OS-X	NO	1	"	"	"	"	"	2	2	2	1	

RACCOMANDAZIONI PER IL PIENO SODDISFACIMENTO DELLA NORMATIVA VIGENTE (D.LGS 30 GIUGNO 2003, N. 196)

AUTENTICAZIONE

- In seguito all'applicazione delle procedure atte a garantire l'aggiornamento periodico delle password dei sistemi Microsoft (Active Directory) e di posta elettronica, si consiglia di codificare ed ufficializzare tali procedure e di estenderle anche agli applicativi sprovvisti (ogni 6 mesi per il trattamento di dati personali ogni 3 mesi in caso di trattamento di dati sensibili e giudiziari).

- Si consiglia di codificate ed ufficializzare le procedure già applicate attraverso le quali il titolare può disporre dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato, in caso di esclusiva necessità.

- Si consiglia inoltre di codificare le procedure già applicate per l'assegnazione delle password amministrative dei sistemi in modo individuale, per poter avere una più corretta tracciabilità delle sessioni sistemistiche.

- Si consiglia di uniformare e di codificare l'accesso a tutti gli applicativi per mezzo dell'autenticazione centralizzata esistente (Active Directory).

- Si consiglia di codificare ed ufficializzare le procedure applicate per la creazione di password conformi ai criteri di complessità stabiliti dalla normativa vigente (almeno 8 caratteri o della lunghezza massima consentita dallo strumento elettronico, alfanumeriche, che non contengano riferimenti riconducibili all'incaricato)

- Si suggerisce di implementare e codificare le procedure per il logout e/o blocco automatico dell'utenza, in caso di allontanamento dell'incaricato dalla postazione di lavoro (Per gli applicativi sprovvisti).

APPLICATIVI

- Si suggerisce di aggiornare gli applicativi che presentano un'inefficienza nel controllo delle viste permesse sui dati, in modo da evitare la visualizzazione di dati non consentiti. E' da segnalare che alcuni sistemi sono stati aggiornati e l'utilizzo degli applicativi è basata sulla profilazione dell'utente, centralizzata in termine di autorizzazioni da un sistema LDAP
- Si consiglia di implementare e codificare procedure di Test degli applicativi prima di distribuirli sul sistema. implementare e codificare procedure di:
    - Test degli applicativi prima di distribuirli sul sistema.
    - Software distribution
    - Gestione delle ripartenze
    - Aggiornamento

SERVER

- Si consiglia di codificare e ufficializzare le soluzioni implementate per il Disaster Recovery del sistema PACS/RIS.

- A seguito dell'implementazione delle soluzioni di Cluster (alta affidabilità) per i sistemi di Backend quali il dominio, la posta elettronica e i server Applicativi, si consiglia di codificare e ufficializzare tali soluzioni.

- Sono stati implementati e codificati sistemi di backup automatico (Time Navigator) che soddisfano i requisiti vigenti.

- Si consiglia di uniformare e codificare le procedure per il ripristino dei dati soggetti a Backup/Restore.

RETE

- Si consiglia di effettuare attività di Vulnerability Assessment/Penetration Test periodiche in modo da verificare ed identificare le vulnerabilità logiche e organizzative, in relazione al networking ed ai sistemi. Un audit specifico e dedicato, con strumenti adeguati, relativo alla sicurezza fisica e logica dei vari aspetti della rete dell'Azienda fornirebbe delle indicazioni precise in merito alle priorità ed aree di intervento.

INFRASTRUTTURA

- Si consiglia di implementare e codificare un sistema di controllo accessi e videosorveglianza adeguato per l'accesso alla Sala Server. Attualmente l'accesso avviene per mezzo di ritiro/restituzione della chiave e controllo visivo in portineria.

ORGANIZZAZIONE

- Si suggerisce di implementare e codificare, di concerto con UUOO Risorse Umane, le procedure per la verifica della sussistenza delle condizioni per la conservazione del profilo di autorizzazione.

SCHEDE DI ANALISI

La strumento utilizzato per il rilevamento dei dati atti alla stesura della presente Analisi dei Rischi è contenuto in una cartella di lavoro in formato Microsoft Excel. Il file, denominato "Matrice_Analisi_Rischi_YY_VerXX" (dove "YY" rappresenta l'anno e "XX" la versione del file) è archiviato e conservato a cura dell'ufficio Sistemi Informativi ed è accessibile/consultabile/modificabile esclusivamente sotto il diretto controllo del personale del medesimo ufficio, su indicazioni del Titolare del trattamento.

Tale cartella presenta singoli fogli di lavoro dedicati, per ciascun ambito interessato dall'analisi (dati, applicativi, server, rete, infrastruttura, organizzazione), nonché il riassuntivo "Cruscotto Generale" così come rappresentato nel presente documento.

I fogli di lavoro racchiudono i dati principali e le informazioni di competenza per ciascun ambito di analisi quali, tra gli altri e a titolo esemplificativo:

- elenco strumenti
- localizzazione
- utilizzo
- ambito operativo (sistemi)
- procedure
- prassi

Nello strumento di analisi si riscontrano alcune sigle relative alle procedure, la chiave di lettura è la seguente:

C A	=	Procedure CODIFICATE ed APPLICATE
nc A	=	Procedure NON codificate ma APPLICATE
C na	=	Procedure CODIFICATE ma NON applicate
na nc	=	Procedure NON codificate e NON applicate

L'aggiornamento della suddetta cartella di lavoro permette la revisione periodica del "Cruscotto Generale" con l'indicazione del valore di rischio per ciascun ambito analizzato e calcolato secondo i criteri precedentemente indicati nel presente documento.

Allegato 3

Elenco Amministratori di sistema

Amministratori di sistema	Società	Ambito di operatività	Sistemi interessati
Andrea Migliaro	Fondazione Besta	Supervisione e Attività sistemistica	DHCP, Dominio, File Server, Server Santer, Server Synapsis, Server EngiSanità, Server EngiModem, Pers_Server, Controllo di Gestione, DominoBesta, Application Server Web Santer, Application Server Web EngiSanità, LIS WINLAB, LIS WINLABWEB, Winlab TESI, Linux_Server, HP MPS CONSOLE nodo A, HP MPS CONSOLE nodo B, HP VPAR1_A_NODO A, HP VPAR2_A_NODO A, HP VPAR3_A_NODO A, HP VPAR4_A_NODO A, HP VPAR1_B_NODO B, HP VPAR2_B_NODO B, HP VPAR3_B_NODO B, HP VPAR4_B_NODO B, HP REPOSITORY REFERTI, HP SISSWAY, HP PKG_SYNAPSIS, HP CUP ONLINE
Paloma Callori	Fondazione Besta	Configurazione utenti	Dominio
Mario Mambretti	Fondazione Besta	Attività sistemistica	DHCP, Dominio, File Server, Server Santer, Server Synapsis, Server EngiSanità, Server EngiModem, Pers_Server, Controllo di Gestione, DominoBesta, Application Server Web Santer, Application Server Web EngiSanità, LIS WINLAB, LIS WINLABWEB, Winlab TESI
Fulvio Croci	Fondazione Besta	Attività sistemistica	DHCP, Dominio, File Server, Server Santer, Server Synapsis, Server EngiSanità, Server EngiModem, Pers_Server, Controllo di Gestione, DominoBesta, Application Server Web Santer, Application Server Web EngiSanità, LIS WINLAB, LIS WINLABWEB, Winlab TESI
Vittorio La Mantia	Sysline (presidio Fondazione Besta)	Attività sistemistica	DHCP, Dominio, File Server, Server Santer, Server Synapsis, Server EngiSanità, Server EngiModem, Pers_Server, Controllo di Gestione, DominoBesta, Application Server Web Santer, Application Server Web EngiSanità, LIS WINLAB, LIS WINLABWEB, Winlab TESI, Linux_Server, HP MPS CONSOLE nodo A, HP MPS CONSOLE nodo B, HP VPAR1_A_NODO A, HP VPAR2_A_NODO A, HP VPAR3_A_NODO A, HP VPAR4_A_NODO A, HP VPAR1_B_NODO B, HP VPAR2_B_NODO B, HP VPAR3_B_NODO B, HP VPAR4_B_NODO B, HP REPOSITORY REFERTI, HP SISSWAY, HP PKG_SYNAPSIS, HP CUP ONLINE
Alessandro Gugliada	Sysline (presidio Fondazione Besta)	Configurazione utenti	Dominio
Diego Gervasoni	Service Trade (presidio Fondazione Besta)	Configurazione utenti	Dominio

Amministratori di sistema	Società	Ambito di operatività	Sistemi interessati
Massimo Cantucci Marco Mercurio Giorgio Falzone Roberto Pirone Andrea Marano Guido Cannito	Tesi	Attività sistemistica, Assistenza remota	LIS WINLAB, LIS WINLABWEB, Winlab TESI
Daniele Paolucci Leonia Burdassi Serena La Manna Pierfrancesco Sormani	Synapsis	Attività sistemistica, Assistenza remota	Server Synapsis, HP PKG_SYNAPSIS
Domenico Alberga Kolibou Alfa Massimo Bellicini Primiano Fede Alessandro Magno Luca Varani Matteo De Matteo Paolo Giannoli Cristiano Zucca Sante Venziani Carlo Maffei Simone Danazzo Elisa Tronconi Zekari Carminati Antonio Fasciano Luigi Gangale Flaviano Sartori Pierluigi Beato Marco Bonetti Paolo Cortese Allan Della Libera Luciano Marenzi Alberto Porta Sergio Punzi Rino Rusconi	Exprivia	Attività sistemistica, Assistenza remota	Server PACS/RIS

Amministratori di sistema	Società	Ambito di operatività	Sistemi interessati
Mirko Grappi Alessio Mugnaioli Fabio Chiazzaro Nazzareno Almonti Primo Angellotti Andrea Assandro Gabriele Belladonna Andrea D'Ambrosio Stefano D'Archivio Alessandro Demetrio Roberta Fortuna Palmiro Macchiati Sammy Magnaguadagno Andrea Palizzi Fabio Ramini Federico Viozzi Alessandro Vita Marco Mella Massimiliano Tora Paola Ceruti Ibrahim Maher Pierluigi Macchi Fabrizio Turturiello Massimo Corradetti Amedeo Tossici	Engisanità	Attività sistemistica, Assistenza remota	Server EngiSanità, Server EngiModem, Application Server Web EngiSanità
Ernesto Goteri Giovanni Civardi Massimiliano Tremolizzo	Archebit	Attività sistemistica, Assistenza remota	Server di Posta
Giovanni Angoli Pacho Baratta Andrea Candian Paolo Conforto Alessandro Favretto Marco Firetti Lucio Lipreri Mauro Migliore Michele Soragni Nicola Masseroni Francesco Meneghetti Aldo Sartori Sergio Cigoli Deborah Ghisolfi Andrea Lazzari Nicola Raschi	Fabbrica Digitale	Attività sistemistica, Assistenza remota	Firewall01, Firewall02, Proxy01, Proxy02, Dominio
Giulio Dei Fabio Giarrizzo	Consorzio Bioingegneria (MT)	Attività sistemistica, Assistenza remota	Server Medical Tutorial

Amministratori di sistema	Società	Ambito di operatività	Sistemi interessati
Cristian Aimi Gianluigi Amoretti Andrea Bettati Gabriele Boni Sandro Cattarinussi Marco Donelli Nicola Farina Alberto Ferrari Maurizio Franceschini Filippo Franchi Sergio Marchini Stefano Marisi Maurizio Monica Marco Orsi Mirko Piola Natascia Poli Milena Soliani Nicola Spotti	Infoline	Attività sistemistica, Assistenza remota	Pers_server
Massimo Di Michele Luca Ghiadoni	GCS	Attività sistemistica, Assistenza remota	DominoBesta
Michele Caspani Sofia Pilon Marco Stellisano Claudio Busoni Salvatore Borrelli Silvia Bragagia Simone Spinosa Davide Selva Fabio Ledda Stefano Rossini Fabio Tango Dario Salvadori Stefano Orlandi Marco Ravagnati Ilaria Marzolla Emanuele Baj	Azienda Ospedaliera Ospedale Niguarda Cà Granda	Attività sistemistica, Assistenza remota	Server Medical Tutorial

Amministratori di sistema	Società	Ambito di operatività	Sistemi interessati
Edoardo Danieli Marco Neritino Laura Gagliardi Stefania Orfanini Anna Magni Luigi Raimondi Claudio Castiglioni Francesco Mangia Luigi Rosario Donnanno Gaetano De Girolamo	Santer	Attività sistemistica, Assistenza remota	Server Santer, Application Server Web Santer, HP VPAR1_A_NODO A, HP VPAR2_A_NODO A, HP VPAR3_A_NODO A, HP VPAR4_A_NODO A, HP VPAR1_B_NODO B, HP VPAR2_B_NODO B, HP VPAR3_B_NODO B, HP VPAR4_B_NODO B, HP REPOSITORY REFERTI, HP SISSWAY, HP CUP ONLINE
Paolo Pierotti Luca Alunni	Themis	Manutenzione, monitoraggio esecuzione back up del database contenente i dati delle cartelle cliniche, referti del vs ospedale Riversamenti diretti dei volumi di conservazione a norma su file system	Sistema Documentale di Conservazione documenti sanitari