ISTITUTO PER LO STUDIO
E LA PREVENZIONE ONCOLOGICA

DELIBERAZIONE DEL DIRETTORE GENERALE
(Nominato con D.P.G.R.T. n. 50 del 28/04/2008)

N° 72 del 31/03/2010

Oggetto: **ISPO – APPROVAZIONE DOCUMENTO PROGRAMMATICO SULLA SICUREZZA ANNO 2010**		
Struttura Proponente	**DIREZIONE AZIENDALE**	
Proposta n.	Responsabile del procedimento	
	Estensore	Dr.ssa Paola Palchetti

IMMEDIATAMENTE ESEGUIBILE [X]

Importo di spesa:

Conto Economico n.

Eseguibile a norma di Legge dal 31 MAR. 2010

Pubblicato a norma di Legge il 31 MAR. 2010

Inviato al Collegio Sindacale il _____

L'anno 2010, il giorno 31 del mese di MARZO
Il sottoscritto Dott.ssa Elena Lacquaniti , nella sua qualità di

DIRETTORE GENERALE

di questo Istituto per lo Studio e la Prevenzione Oncologica , con sede in Via Cosimo Il Vecchio 2 – 50139 Firenze, in forza del Decreto del Presidente della Giunta Regionale Toscana n. 50 del 28/04/2008.

Visto il D. Lgs.vo 30/12/1992 n. 502 e sue successive modifiche ed integrazioni e la L. R. Toscana n. 40 del 24/02/2005 di disciplina del Servizio Sanitario Regionale e successive modificazioni ed integrazioni;

Vista la LRT 4 febbraio 2008, n. 3 recante " Istituzione e organizzazione dell'Istituto per lo Studio e la Prevenzione Oncologica (ISPO) Gestione liquidatoria del Centro per lo Studio e la Prevenzione Oncologica ";

Dato atto che in forza della Legge RT 4 febbraio 2008, n. 3 l'Istituto per lo Studio e la Prevenzione Oncologica (ISPO) è Ente del Servizio Sanitario Regionale, dotato di personalità giuridica pubblica e di autonomia organizzativa, amministrativa e contabile e subentra nelle attività esercitate dal disciolto CSPO a far data dal 1 Luglio 2008;

Vista la delibera del Direttore Generale n° 5 del 14.07.2008 con la quale è stato approvato il regolamento dell'Ispo;

Visto il Decreto Legislativo n. 196 del 30.06.2003 *"Codice in materia di protezione dei dati personali"*

Considerato che, ai sensi dell'art. 34 del D.Lgs. 196/2003, i titolari del trattamento sono tenuti ad adottare misure minime di sicurezza volte ad assicurare un livello minimo di protezione dei dati personali ed a certificarne e pianificarne l'implementazione attraverso la predisposizione di un *Documento programmatico sulla sicurezza;*

Considerato altresì che il Disciplinare tecnico unito quale Allegato B al D.Lgs. 196/2003 prevede, al punto 19, la redazione e l'aggiornamento del *Documento programmatico sulla sicurezza* entro il 31 marzo di ogni anno;

Preso atto inoltre che il suddetto Disciplinare tecnico prevede, al punto 26, che il titolare riferisca, nella relazione accompagnatoria del bilancio d'esercizio, dell'avvenuta redazione o aggiornamento del Documento programmatico sulla sicurezza;

Dato atto che dall'1.7.2008 ISPO, in qualità di Titolare del Trattamento dei dati, ed in persona del Direttore Generale nonché Rappresentante Legale dell'Istituto ha provveduto, in conformità ai principi e agli obblighi fissati dal Codice, ad adottare gli interventi necessari per garantire una idonea gestione ed organizzazione dei trattamenti dei dati personali trattati da ISPO;

Richiamata la deliberazione del Direttore Generale n. 53 del 31. 03.2009 con la quale si provvede all'approvazione del Documento Programmatico sulla sicurezza per l'anno 2009;

Visto il Documento Programmatico sulla Sicurezza che, come allegato di lettera A si ritrova unito alla presente deliberazione a farne parte integrante e sostanziale, comprensivo dell'Allegato sub 1 "Elenco dei trattamenti e dei Responsabili per aree di attività";

Ritenuto pertanto opportuno procedere all'approvazione dell'atto sopracitato, quale documento di riferimento da applicare a tutte le strutture dell'Istituto;

Dato atto che il documento allegato ha validità a decorrere dalla data di approvazione e sarà oggetto, entro il 31 marzo dell'anno successivo a quello di approvazione, di revisione per adeguarlo ad eventuali variazioni intervenute sia per quanto riguarda compiti e responsabilità dei trattamenti, sia per quanto riguarda il livello di rischio cui sono soggetti i dati personali, al fine di individuare le misure di sicurezza da adottare per la tutela degli stessi;

Ravvisata la necessità di dichiarare il presente provvedimento immediatamente esecutivo ai sensi della normativa in materia, al fine di consentirne l'immediata applicazione;

Acquisito il visto di conformità giuridico amministrativa del Coordinatore Amministrativo;

Con il parere favorevole del Direttore Sanitario;

DELIBERA

per i motivi espressi in narrativa:

1) di procedere all'approvazione e sottoscrizione del "Documento Programmatico sulla sicurezza dei dati dell'Istituto per lo Studio e la Prevenzione Oncologia (ISPO) per l'anno 2010 che si ritrova unito, quale allegato di lettera "A", al presente decreto a farne parte integrante e sostanziale;

2) di trasmettere la presente deliberazione a tutti i Responsabili UU.OO.

3) di dare notizia dell'adozione del Documento Programmatico della sicurezza nella relazione di accompagnamento al bilancio d'esercizio;

4) di dichiarare il presente atto immediatamente esecutivo ai sensi della normativa vigente;

5) di trasmettere il presente atto all'Albo di pubblicità degli atti di questo Istituto per lo Studio e la Prevenzione Oncologica e al Collegio Sindacale.

IL DIRETTORE GENERALE
(Dott.ssa Elena Lacquaniti)

IL DIRETTORE SANITARIO
(Carolina Cuzzoni)

ELENCO DEGLI ALLEGATI

ALLEGATO "A" ALLA DELIBERA D.G. N. 72
del 31/03/2010

Istituto per lo Studio e la Prevenzione Oncologica

Documento programmatico sulla sicurezza dei dati per l'anno 2010

(ai sensi dell'Allegato B al D. Lgs. 30 giugno 2003, n. 196)

INDICE

1. Introduzione 4
1.1 Approvazione 4
2. Scopo del documento 4
2.1. Applicabilità 4
2.2. Revisione del documento 4
2.3. Riferimenti normativi 4
2.4. Definizioni 5
2.5. Classificazione dei dati e caratteristiche dei trattamenti 7
3. Distribuzione dei compiti e delle responsabilità 8
3.1. Titolare del trattamento 8
3.2. Responsabili ed incaricati dei trattamenti 9
3.3. Sistema informatico ISPO 9
3.4. Amministrazione delle funzioni di sicurezza per il sistema informatico ISPO 12
4. Analisi dei rischi 12
4.1. Rischi specifici 12
4.2. Rischi sull'integrità dei dati 13
4.3. Rischi sulla riservatezza dei dati 13
4.4. Rischi sulla disponibilità dei dati 14
4.5 Rischi di trattamento non conforme alle finalità della raccolta 14
4.6 Contromisure adottate 14
5. Protezione delle aree e dei locali 16
5.1. Criteri generali 16
5.2. Procedure di accesso agli edifici ed ai locali interni 16
5.3. Procedure di accesso alle sale macchine e apparati di controllo ambientale 16
6. Misure per garantire l'integrità dei dati 17
6.1. Criteri generali 17
6.2. Sistema di autorizzazione degli utenti 17
6.3. Sistema di autenticazione degli utenti 17
6.3.1. Autenticazione per l'accesso alla rete locale 17
6.3.2. Autenticazione per l'accesso agli applicativi 18
6.4. Misure di prevenzione di intrusioni e azioni di programmi ostili 18
6.5. Misure di prevenzione di accessi abusivi e vulnerabilità degli strumenti 19
7. Misure per garantire il ripristino della disponibilità dei dati 19
7.1. Salvataggio dei dati 19
7.2. Procedure di ripristino dei dati 19
8. Criteri per il trattamento di dati all'esterno della struttura 20
8.1. Norme di sicurezza 20
8.2. Separazione delle responsabilità / attività di sicurezza 20
8.3. Standard di sicurezza di tutti i servizio dati in *outsourcing* 20
8.4. Isolamento della rete/LAN 20
8.5. Controlli e *Audit* 20
9. Criteri per il trattamento dei dati sanitari 21
9.1. Misure di sicurezza per dati trattati in elenchi, registri o banche dati 21
10. 1. Informazione e formazione 23
1. Trattamento dei dati personali in ambito sanitario 25
11. Verifiche periodiche 26

Parte Prima

Quadro di riferimento

1. Introduzione

1.1 Approvazione

Il presente documento è stato approvato dal Direttore Generale dell'Istituto per lo Studio e la Prevenzione Oncologica, Istituto Scientifico della Regione Toscana (di seguito detto anche "ISPO" o l'"Istituto")

Data **Firma**

2. Scopo del documento

Scopo di questo documento è di stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi previsti dal D.Lgs. 30 giugno 2003, n. 196 *Codice in materia di protezione dei dati personali* (di seguito anche D. Lgs. 30 giugno 2003 N. 196, D. Lgs. 196/03 o *Codice*) e dal relativo disciplinare tecnico in materia di misure minime di sicurezza (allegato B).

2.1. Applicabilità

Il presente documento si applica a tutte le strutture di ISPO. Si precisa che l'analisi è stata estesa, in via generale, a tutti i trattamenti, indipendentemente dalle circostanze operative che rendono necessario l'obbligo di compilazione del Documento Programmatico sulla Sicurezza ai sensi del paragrafo 19 dell'allegato B del Codice privacy.

2.2. Revisione del documento

Il presente documento ha validità a decorrere dalla data di approvazione.

Entro il 31 Marzo dell'anno successivo a quello di approvazione e così per gli anni successivi, il documento sarà oggetto di revisione per adeguarlo ad eventuali variazioni intervenute sia per quanto riguarda compiti e responsabilità dei trattamenti sia per quanto riguarda il livello di rischio cui sono soggetti i dati personali, al fine di individuare le misure di sicurezza da adottare per la tutela degli stessi.

2.3. Riferimenti normativi

D. Lgs. 196 del 30 giugno 2003 *Codice in materia di protezione dei dati personali* e successive modifiche ed integrazioni (di seguito *Codice*), compreso il relativo Allegato B *Disciplinare tecnico in materia di misure minime di sicurezza* (di seguito Allegato B al *Codice*)
Dipartimento della funzione pubblica - Direttiva 1/2005 Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196 ... con particolare riguardo alla gestione delle risorse umane
Regione toscana - Delibera Giunta Regionale 29 novembre 2004 Linee guida alle Aziende sanitarie per l'applicazione del Codice
Regione toscana - Decreto del Presidente della Giunta regionale 16 maggio 2006: Regolamento per il trattamento dei dati sensibili e giudiziari da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo

Autorità Garante per la Protezione dei dati personali:

Provvedimento generale - *Lavoro: le linee guida del Garante per posta elettronica e internet* (Gazzetta Ufficiale n. 58 del 10 marzo 2007)
Provvedimento - *Internet: proporzionalità nei controlli effettuati dal datore di lavoro - 2 febbraio 2006*
Provvedimento del 18 maggio 2006
Provvedimento - *Limiti al controllo sulla posta elettronica del dipendente - 2 aprile 2008*
Parere del 22 marzo 2004 - Obblighi di sicurezza e documento programmatico
Guida operativa per redigere il Documento programmatico sulla sicurezza - 11 giugno 2004
Provvedimento: Videosorveglianza - 29 aprile 2004
Provvedimento: Strutture sanitarie: rispetto della dignità - 9 novembre 2005
Autorizzazione al trattamento dei dati genetici - 22 febbraio 2007
Provvedimento: Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico - 14 giugno 2007
Provvedimento: Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali – 24 luglio 2008
Differimento dell'efficacia dell'autorizzazione al trattamento dei dati genetici rilasciata il 22 febbraio 2007 - 19 dicembre 2008
Provvedimento: Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008
Provvedimento: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008;
Provvedimento: Proroga delle misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 12 febbraio 2009;
Provvedimento: Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009.
Provvedimento: Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009
Provvedimento: Linee guida in tema di referti on-line - 19 novembre 2009

Gruppo di lavoro ex articolo 29 direttiva 95/46/CE:
Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE) adottato il 15 febbraio 2007
Parere 4/2007 sul concetto di dati personali adottato il 20 giugno 2007

2.4. Definizioni

Dati personali: qualunque informazione relativa ad un soggetto - persona fisica, persona giuridica, ente od associazione - identificato o identificabile (anche indirettamente, mediante riferimento a qualsiasi altra informazione, compreso un numero di identificazione personale).
Dati anonimi: i dati che, in origine o a seguito di trattamento, non possono essere associati ad un interessato, appunto, identificato o identificabile.
Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Dati giudiziari: i dati personali idonei a rivelare provvedimenti 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.
Dati genetici: tutti i dati, indipendentemente dalla tipologia, che riguardano i caratteri ereditari di un individuo o le modalità di trasmissione di tali caratteri nell'ambito di un gruppo di individui legati da vincoli di parentela.

Documento analogico: il documento formato utilizzando una grandezza fisica che assume valori continui, ad es. il documento cartaceo; il documento analogico si distingue in originale e copia (il documento analogico originale può a sua volta essere unico oppure non unico: si dice non unico qualora sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi, come nel caso delle fatture).
Documento informatico: il documento formato tramite una grandezza fisica che assume valori binari, ottenuti attraverso un processo di elaborazione elettronica.
Trattamento: qualunque operazione o complesso di operazioni effettuato sui dati personali (raccolta, registrazione, organizzazione, conservazione; consultazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco comunicazione, diffusione, cancellazione, distruzione di dati). Rientrano nella nozione di trattamento anche le operazioni effettuate senza l'ausilio di strumenti elettronici, nonché quelle relative ad informazioni non organizzate in banche dati.
Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati (diversi dall'interessato, dal responsabile e dagli incaricati), in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Titolare: il soggetto - persona fisica, persona giuridica, pubblica amministrazione o qualsiasi altro ente, associazione od organismo - cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso.
Responsabile: il soggetto - persona fisica, persona giuridica, Pubblica Amministrazione o qualsiasi altro ente, associazione od organismo - preposto dal titolare al trattamento di dati personali.
Incaricato: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile, in pratica chi materialmente effettua le operazioni di trattamento di dati.
Amministratori di sistema: gli incaricati della gestione e manutenzione di un impianto di elaborazione o di sue componenti, oppure della amministrazione di basi di dati, di reti e di apparati di sicurezza, di sistemi software complessi.
Interessato: il soggetto (persona fisica, persona giuridica, ente o associazione) cui si riferiscono i dati personali.
Garante per la Protezione dei dati personali: organo collegiale che ha tra l'altro il compito di:

- controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile;
- esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati;
- prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;
- vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco;
- promuovere la sottoscrizione di codici deontologici;
- esprimere pareri nei casi previsti.

Referente Aziendale per la Privacy: la persona fisica, nominata con atto del Direttore Generale su proposta del Direttore Amministrativo, che svolge i seguenti compiti:

- garantisce il supporto alla Direzione Aziendale nei rapporti con il Garante e nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia, segnatamente in tema di notificazione al Garante ex art. 37 del Codice e comunicazioni al Garante ex art. 39 del Codice;
- collabora alla stesura del Documento Programmatico sulla Sicurezza avvalendosi dell'apporto dei Responsabili del trattamento;
- vigila sull'osservanza del Regolamento aziendale sulla privacy;
- tiene ed aggiorna il Censimento dei trattamenti, sulla base delle comunicazioni effettuate dai Responsabili del trattamento;
- tiene e aggiorna l'elenco completo dei Responsabili del trattamento in ambito aziendale, sulla base delle informazioni inviategli dalle strutture competenti;

- tiene ed aggiorna l'elenco degli archivi cartacei e/o magnetici contenenti dati personali custoditi a livello aziendale;
- propone, svolge e/o coordina l'attività di formazione in tema di normativa sulla riservatezza dei dati, assicurando la promozione della cultura della privacy a livello aziendale;
- supporta le strutture aziendali nella gestione dei riscontri alle istanze degli interessati ex art. 7 del Codice, e si attiva per comporre le controversie sui dati personali;
- fornisce la necessaria consulenza in ordine alle problematiche in tema di riservatezza;
- propone l'adeguamento dei percorsi e delle procedure aziendali per quanto attiene l'aspetto della riservatezza dei dati;
- si occupa dei conflitti tra diritto alla riservatezza dei dati e dovere di garantire la trasparenza dell'attività amministrativa.

2.5. Classificazione dei dati e caratteristiche dei trattamenti

Al fine di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti degli interessati, ISPO ha attivato un processo di classificazione e rilevazione delle banche dati, per le quali assume la qualifica di "Titolare", ai sensi del D. Lgs. 30 giugno 2003, N. 196

In particolare sono state censite le banche dati, sono stati descritti, a livello informatico, i processi di lavoro, sono state verificate tutte le misure di sicurezza poste a tutela dei singoli trattamenti o dati, sono stati individuati i soggetti fisici e giuridici abilitati alle diverse operazioni di trattamento ed è stato esaminato il Regolamento interno (Statuto) dell'ISPO.

Tale attività è stata svolta analizzando sia i trattamenti effettuati con l'ausilio di mezzi elettronici, sia quelli su supporto cartaceo; per ogni trattamento, indipendentemente dalle modalità di lavorazione, sono state individuate le misure di sicurezza poste in essere, individuando la loro corrispondenza o meno con quanto previsto dall'Allegato B del D. Lgs. 30 giugno 2003, N. 196.

I dati oggetto dei trattamenti sono riconducibili alle seguenti due macro categorie di dati:

- Dati che identificano soggetti fisici (dati anagrafici, dati familiari, ecc), comprensivi di dati sensibili (stato di salute, adesione a sindacati, ecc), ivi inclusi, in alcuni casi, anche dati giudiziari (provvedimenti giudiziari a carico degli interessati).

- Dati relativi a soggetti giuridici (denominazione, ragione sociale, ecc), principalmente di natura commerciale e relativi all'esistenza di obblighi contrattuali o normativi.

I soggetti interessati cui i dati si riferiscono possono essere classificati nelle seguenti categorie:

- Pazienti
- Dipendenti
- Fornitori
- Outsourcer

I trattamenti analizzati ricomprendono tanto quelli svolti dall'ISPO per finalità istituzionali ed in esecuzione di obblighi normativi, quanto quelli effettuati sulla base di obblighi contrattuali assunti dall'Istituto con terzi.

Il trattamento dei dati avviene tanto su supporti magnetici, la cui organizzazione è automatizzata, che su supporti cartacei, organizzati in forma non automatizzata.

Le principali finalità di trattamento effettuato dall'ISPO attengono all'esecuzione di attività diagnostico-assistenziali e di ricerca scientifica, ovvero:

- **Ricerca, valutazione epidemiologica e interventi nel campo della prevenzione primaria dei tumori (studi di cancerogeni ambientali e professionali, abitudini alimentari, ecc...);**
- **Ricerca e valutazione nel campo della prevenzione secondaria dei tumori (programmi di screening oncologici);**
- **Assistenza sanitaria e psicologica, riabilitazione e *follow-up* in favore dei pazienti affetti dalle principali neoplasie;**
- **Iniziative di informazione ed educazione alla salute;**
- **Attività di formazione e aggiornamento nell'ambito della prevenzione primaria e secondaria dei tumori;**
- **Gestione dell'attività di screening oncologico in convenzione con aziende sanitarie locali;**
- **Diagnosi delle patologie genetiche (test diagnostici)**
- **Ricerca statistica**

In particolare, ISPO svolge le seguenti attività di interesse regionale:

- **Funzioni di Centro di Riferimento Regionale (CRR) per la prevenzione oncologica;**
- **Attività di ricerca epidemiologica di interesse regionale in campo oncologico.**
- **gestione del Registro Tumori Toscano e del Registro di Mortalità Regionale;**
- **gestione delle Mappe di rischio oncogeno in ambito lavorativo;**
- **gestione del Registro Dializzati sul territorio regionale;**
- **allestimento del Centro Operativo Regionale per i tumori professionali;**
- **allestimento del Centro di Sorveglianza dei tumori eredo familiari**
- **progetto di prevenzione primaria**
- **attivazione del Centro Regionale di Riabilitazione Oncologica**
- **sperimentazione clinica e attività formative rivolte alle strutture afferenti all'Istituto Tumori Toscano**

L'elenco delle banche dati ISPO e dei trattamenti di dati ad esse correlate è allegato al presente documento sotto il numero "**1**". L'aggiornamento del suddetto allegato è a cura del "Referente Privacy" dell'ISPO.

3. Distribuzione dei compiti e delle responsabilità

E' stata esaminata la distribuzione dei compiti e delle responsabilità relativamente al trattamento dei dati personali, con particolare riguardo ai trattamenti svolti con mezzi elettronici o comunque automatizzati.

Si precisa che, per quanto riguarda il settore amministrativo, le varie competenze vengono gestite da ISPO in sinergia con l'Azienda Sanitaria di Firenze.

3.1. Titolare del trattamento

ISPO si qualifica q2uale Titolare del trattamento ai sensi dll'art. 28 del D.Lgs. 196/2003

La struttura organizzativa dell'Istituto prevede al vertice la figura del Direttore Generale deputato al coordinamento delle attività dei diversi responsabili di funzione (U.O.), ivi inclusa quella del responsabile della funzione dei Sistemi Informativi. Si rappresenta, di seguito, l'organigramma aggiornato dell'Istituto,

Segue:

Organigramma Gerarchico Funzionale

3.2. Responsabili ed incaricati dei trattamenti

ISPO, in qualità di Titolare dei dati ai sensi dell'art. 28 del D.Lgs. 196/2003, in seguito alla valutazione della complessità dell'organizzazione aziendale, verificata in particolare l'esistenza di processi aziendali e funzioni quanto mai eterogenee, considerata, inoltre, la necessità di avere un'azione coordinata e sinergica per quanto attiene l'attuazione delle disposizioni previste dal Codice, ha ritenuto di procedere alla nomina di un Responsabile del trattamento dei dati (art. 29 del D.Lgs. 196/2003) per ciascuna area operativa, come indicato nell'allegato 1.

I compiti di ciascun Responsabile del trattamento sono principalmente i seguenti:

- sovrintendere a tutte le operazioni di trattamento di dati personali, comuni e sensibili, effettuati all'interno della propria funzione;
- curare le operazioni di classificazione analitica delle banche dati e dei processi aziendali;
- nominare gli incaricati al trattamento dei dati personali;
- curare l'attuazione delle misure di sicurezza e del loro periodico aggiornamento;
- curare la formazione e l'aggiornamento degli incaricati del trattamento dei dati personali;

Ai Responsabili è richiesto di vigilare sul trattamento dei dati ricompresi nelle attività della propria area di competenza, in modo che esso sia effettuato esclusivamente per lo svolgimento delle mansioni attribuite, in modo lecito e secondo correttezza, nonché di impartire e specificare le istruzioni ricevute dal Titolare sull'accesso e sul trattamento a tutti gli Incaricati che operano sotto la propria responsabilità.

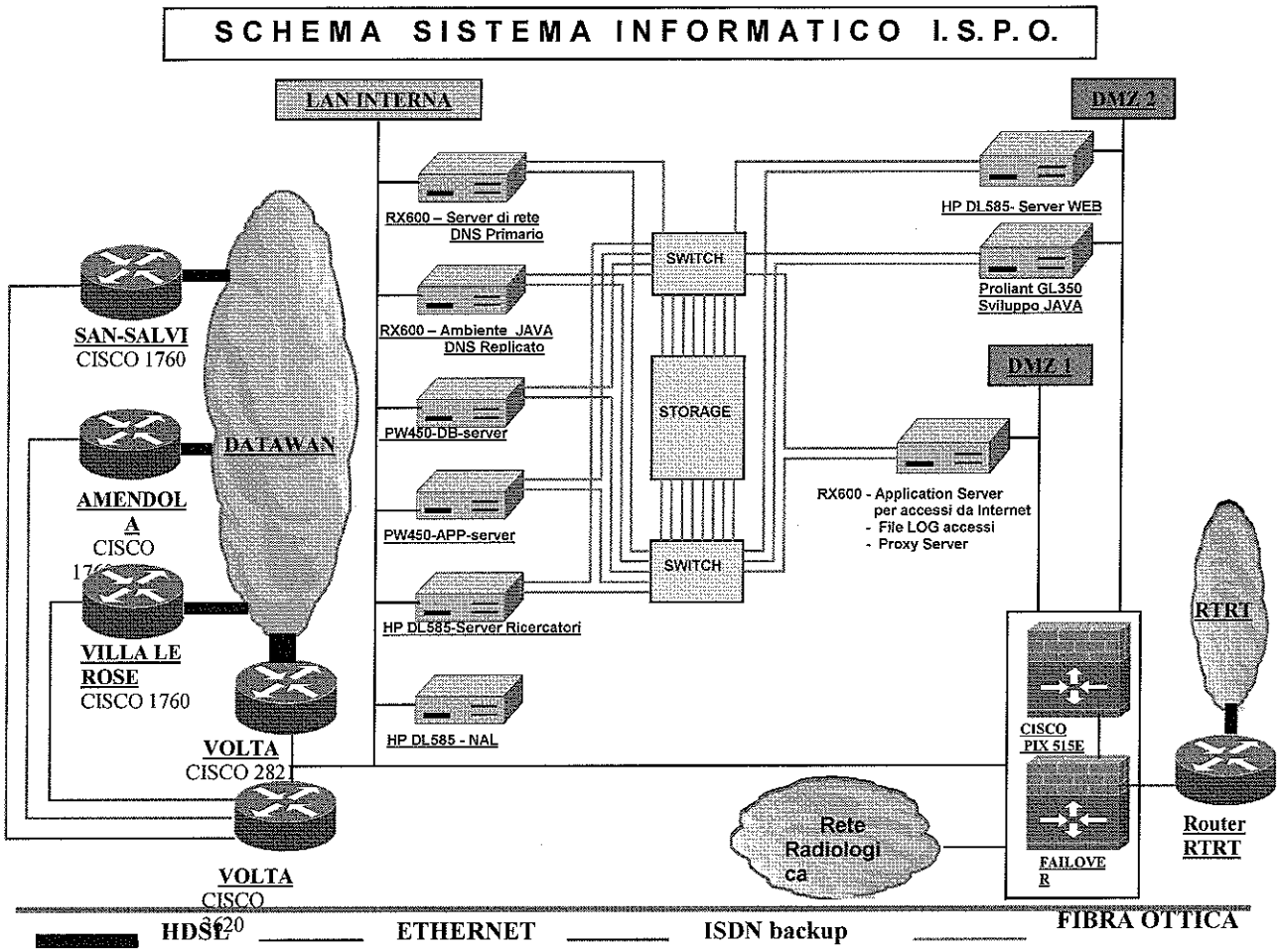
A seguito dell'analisi delle banche dati presenti nei diversi uffici e sulla base dell'individuazione delle effettive operazioni di trattamento effettuate da ciascuno, sono stati formalmente nominati gli Incaricati del trattamento dei dati personali, tramite apposita lettera di nomina firmata per ricevuta ed integrale accettazione da parte dell'Incaricato stesso; il soggetto designato è incaricato a compiere unicamente le attività necessarie per l'espletamento delle sue funzioni e deve attenersi alle specifiche istruzioni impartite dal Titolare e dal Responsabile.

Gli Incaricati del trattamento (art. 30 del D.Lgs. 196/2003), nell'ambito delle mansioni assegnate, hanno le seguenti responsabilità:

- svolgere attività conformi al D.Lgs. N. 196/03;
- svolgere le operazioni di trattamento secondo le direttive del titolare e del responsabile;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento;
- rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile o l'amministratore dei sistemi informatici in caso di incidente di sicurezza che coinvolga dati personali o informazioni in genere;

3.3. Sistema informatico ISPO

L'ISPO si avvale di un Sistema proprio, strutturato su un complesso di server con ambiente UNIX, LINUX, WINDOWS.
Tutte le Sedi sono collegate mediante linee HDSL e ISDN di backup.
L'applicativo per l'utilizzo di office automation è MICROSOFT OFFICE.
La configurazione del Sistema e della rete è schematizzata nella figura seguente:



Il Responsabile del Sistema Informativo ha il compito di garantire lo sviluppo e la gestione di un supporto informatico alle attività dell'Istituto.

Con l'obiettivo di una adeguata protezione del patrimonio informativo dell'Istituto, sono state definite norme comportamentali a cui tutto il personale dell'Istituto deve attenersi. Citiamo di seguito le principali:

- I dipendenti ed il personale dell'Istituto sono tenuti a mantenere riservate (e a prendere adeguati provvedimenti per mantenere riservate) tutte le informazioni riguardanti l'azienda ed i suoi utenti;
- I dipendenti ed il personale dell'Istituto devono fare tutto quanto necessario per garantire la sicurezza dei dati e rispettare le misure di sicurezza adottate;
- I dipendenti ed il personale dell'Istituto possono utilizzare le informazioni ed i sistemi informativi solo per gli appropriati scopi di lavoro e non per uso personale;
- La credenziale di autenticazione è strettamente personale e non può essere utilizzata da terzi;

- La componente riservata della credenziale di autenticazione deve essere scelta in modo tale da essere difficilmente individuabile:
    - Deve essere costituita da un minimo di 8 caratteri.
    - Deve contenere sia caratteri alfabetici che numerici;
    - Non deve essere assolutamente divulgata;
    - Non deve avere riferimenti personali;
- La componente riservata della credenziale di autenticazione deve essere sostituita almeno ogni 3 mesi;
- Qualora la componente riservata della credenziale di autenticazione non dovesse più essere riconosciuta dai sistemi o dovesse essere dimenticata, sarà necessario richiedere al responsabile del Sistema Informativo la cancellazione di quella esistente e la possibilità di inserirne una nuova;
- Qualora si dovesse lasciare incustodita la propria postazione di lavoro chiudere le sessioni di lavoro eventualmente aperte e utilizzare un blocco dello schermo protetto da password;
- Il personale dell'Istituto è responsabile dei salvataggi delle informazioni residenti sulle apparecchiature informatiche assegnate;
- Non è consentito l'utilizzo di prodotti software non ufficialmente rilasciati o acquisiti dall'Istituto;
- Tutto il nuovo software e hardware deve essere installato dalla U.O. Sistema Informativo – EDP;
- Il personale dell'Istituto deve proteggere in modo adeguato i supporti removibili di memorizzazione che contengano informazioni riservate, conservandoli in un ufficio chiuso a chiave o in un armadio chiuso a chiave o in un cassetto chiuso a chiave, accessibili solo da parte soggetti appositamente autorizzati;
- Il reimpiego dei supporti di memorizzazione removibili che contengono informazioni riservate, deve avvenire solo a condizione che il contenuto precedente non sia recuperabile;
- Il personale del Centro deve gestire documenti cartacei che contengono informazioni riservate con estrema cautela, assicurandosi che siano utilizzati in luoghi tenuti sotto controllo, l'accesso ai quali sia limitato al personale che ha una specifica esigenza di lavoro per accedervi;
- Per la custodia dei documenti contenenti informazioni riservate, il personale dell'Istituto deve archiviare la documentazione di propria competenza, assicurandone la conservazione in modo da prevenire smarrimenti o deterioramenti;
- Non è consentito lasciare fogli e documenti contenenti informazioni riservate incustoditi e di conseguenza accessibili da persone estranee non autorizzate all'accesso alle informazioni;
- Tutte le connessioni dall'esterno via modem devono essere esplicitamente autorizzate dall'U.O. Sistema Informativo – EDP;
- Il personale è tenuto ad avvisare il Responsabile dall'U.O. Sistema Informativo – EDP tutte le volte che vengono rubati, smarriti o danneggiati materiali IT o informazioni appartenenti all'Istituto;
- Ogni abuso o utilizzo non conforme alle disposizioni del presente documento o del D.Lgs. 196/2003, dell'accesso ai sistemi informativi e dei dati in essi contenuti, potrà essere perseguito e sanzionato a norma di legge.

Il Responsabile EDP, al fine di implementare il sistema di sicurezza, stabilisce un proficuo e continuo rapporto con i Responsabili delle altre strutture operative.

3.4. Amministrazione delle funzioni di sicurezza per il sistema informatico ISPO

I compiti relativi all'amministrazione della sicurezza del sistema informatico ricadono nelle responsabilità sia della funzione "Sistemi Informativi" dell'Istituto per la gestione della rete interna, sia dell'*outsourcer*, ditta incaricata della gestione Sala Macchine per quanto riguarda la sicurezza fisica e logica dei sistemi ad esso demandati. Tra i compiti di amministrazione della sicurezza dei sistemi rientrano:

- le politiche per il controllo degli accessi ai dati;
- l'individuazione e la protezione delle risorse (dischi, database, ecc.) in accordo con le politiche di sicurezza e gli standard;
- l'attribuzione a ciascun utente per l'accesso al server di un codice identificativo personale ("user-id") e di una parola chiave individuale ("password");
- la definizione, in accordo con le politiche di sicurezza vigenti ed i ruoli aziendali presenti, dei profili di autorizzazione utente per l'accesso agli elaboratori ed ai dati;
- l'associazione "utente-profilo d'autorizzazione";
- la scelta dei programmi "antivirus" per le varie piattaforme elaborative e degli aggiornamenti che si rendono necessari nel tempo;
- le politiche di back-up e di ripristino dei dati;
- la predisposizione di misure di sicurezza logica e fisica per la protezione da distruzione, perdita, manipolazione o riproduzione non autorizzata dei dati.

4. Analisi dei rischi

L'analisi dei rischi è stata condotta in considerazione delle previsioni degli artt. 15 e 31 del Codice in materia di protezione dei dati personali e del richiamato art. 2050 del codice civile, focalizzandosi dunque sulle circostanze possibili o probabili che possano comportare:

1. rischi specifici;
2. rischi sull'integrità dei dati;
3. rischi sulla riservatezza dei dati;
4. rischi sulla disponibilità dei dati;
5. rischi di trattamento non conforme alle finalità della raccolta.

4.1. Rischi specifici

Nella categoria dei rischi specifici sono stati compresi tutti quei rischi che generalmente non trovano una valida protezione nei sistemi di difesa classici: in particolare sono state analizzate tutte le minacce derivanti dalla collocazione territoriale degli uffici dell'ISPO, cioè dall'ubicazione dei luoghi in cui vengono custoditi i dati e svolte le diverse operazioni di trattamento.

Per quanto riguarda il centro elaborazione dati dell'ISPO, si è riscontrato che lo stesso è ubicato in una fascia territoriale geografica che nelle carte di pericolosità sismica non risulta classificata tra le zone a grado di pericolosità medio o elevato: pertanto, non si è ritenuto necessario adottare ulteriori misure di sicurezza per gli edifici, né per garantire la continuità di approvvigionamento dei diversi servizi a tutela dei trattamenti e delle banche dati (telecomunicazioni, energia elettrica, ecc.). Inoltre nelle vicinanze non risultano essere presenti insediamenti di impianti industriali o altre installazioni di aziende che svolgono attività pericolose.

Anche per quanto riguarda le banche dati presenti presso le sedi distaccate dell'ISPO, non sono stati rilevati particolari problemi di natura sismica o comunque legati alla morfologia del territorio, per cui non risultano rischi specifici prevedibili e probabili che richiedano particolari cautele.

4.2. Rischi sull'integrità dei dati

L'accertamento dell'integrità dei dati ha riguardato la protezione dei medesimi dai rischi di possibili modifiche o distruzioni accidentali o deliberate: tali rischi possono essere, pertanto, classificati in: **I)** rischi di carattere accidentale, **II)** rischi di carattere volontario e **III)** rischi da programmi pericolosi.
I dati personali trattati da ISPO sono conservati sui server, come descritto nel precedente capitolo, e su cassette di *backup* opportunamente custodite.
Ciascuna Unità Operativa\Ufficio è considerata proprietaria convenzionale dei dati che tratta e, conseguentemente, è ritenuta responsabile della loro tutela, quale patrimonio dell'Istituto, e della scrupolosa osservanza delle norme di trattamento, archiviazione e rispetto delle limitazioni di accesso, avendo come obiettivo la sicurezza dei dati, in modo da:

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

I rischi di carattere accidentale riguardano l'involontaria sovrascrittura o distruzione dei dati imputabile ad azioni umane errate quali, ad esempio, comandi applicativi od operativi errati oppure a malfunzionamenti hardware o guasti delle apparecchiature dedicate alla memorizzazione.

I rischi di carattere volontario fanno, invece, riferimento alle alterazioni dell'integrità dei dati conseguenti ad un'azione deliberatamente perpetrata allo scopo di modificare volontariamente i dati, inserire nuovi dati o distruggere quelli presenti.

Infine, i rischi connessi alla diffusione di virus e programmi di cui all'art. 615 *quinquies* del codice penale riguardano la corruzione dei file eseguibili, corruzione dei dati, perdita di file, perdita di spazio utilizzabile nelle memorie, malfunzionamenti del sistema, degrado delle prestazioni del sistema, impossibilità di utilizzo del sistema, ecc. I virus ed i programmi pericolosi potrebbero penetrare nei computer tramite supporti infettati provenienti da terzi, supporti infettati importati dai dipendenti senza autorizzazione, file scambiati in rete, ecc.

4.3. Rischi sulla riservatezza dei dati

Per quanto attiene la riservatezza dei dati si è fatto riferimento alla natura ed al grado di confidenzialità, riservatezza e particolarità dei dati, al fine di garantire la dovuta necessaria riservatezza delle informazioni proteggendole da ipotetiche divulgazioni non autorizzate e consentendone l'utilizzo ed il trattamento solamente ai soggetti fisici incaricati.

Tale rischio è stato esaminato in relazione alla possibilità che si realizzino rilasci di informazioni non autorizzate e/o accessi non consentiti ai dati. In particolare si possono distinguere rischi di accessi fraudolenti dall'interno e rischi di accessi fraudolenti dall'esterno.

I rischi di accessi non consentiti dall'interno possono essere dovuti a diverse cause: profilo di autorizzazione all'accesso non aderente al ruolo assegnato o conseguente all'attribuzione di privilegi di accesso eccessivi; utilizzo dei privilegi di amministratore di sistema; impersonificazione di un dipendente autorizzato all'accesso ai sistemi; manomissione delle autorizzazioni da parte del personale addetto al controllo ed all'amministrazione dei profili di accesso; cattura di informazioni utili che correlate tra loro consentono di giungere alla conoscenza indiretta dei dati.

Per quanto riguarda, invece, i rischi di accesso non consentiti dall'esterno, essi possono essere conseguenti ad accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software, ad impersonificazione di un dipendente autorizzato all'accesso remoto ai sistemi, ad intercettazione di comunicazioni telematiche.

4.4. Rischi sulla disponibilità dei dati

La disponibilità dei dati si riferisce alla necessità ed al conseguente diritto dei soggetti interessati che i dati personali possano essere utilizzati in tutte le forme e le circostanze previste, per cui è necessario fare in modo che i dati siano disponibili al momento di una richiesta effettuata dal personale in possesso delle autorizzazioni necessarie. I rischi di non disponibilità sono stati esaminati in relazione ad eventi di natura accidentale o intenzionale.

I rischi di carattere accidentale fanno riferimento all'eventualità che le informazioni non siano disponibili a causa di eventi non volontari e/o non previsti dovuti a varie cause: anomalie in programmi che avrebbero dovuto elaborare i dati e che non hanno potuto completare la loro esecuzione; errate azioni del personale incaricato che impediscono l'accesso alle informazioni; malfunzionamenti o guasti hardware; dimensionamento insufficiente delle risorse tecnologiche dedicate alla trasmissione ed alla memorizzazione.

I rischi di carattere intenzionale riguardano i casi in cui le informazioni non sono disponibili a causa di azioni umane volontarie, poste in essere con lo scopo preciso e determinato di impedire l'accesso alle informazioni da parte dei soggetti che detengono il pieno diritto di farlo. Tali minacce sono relazionate principalmente a generica negligenza e/o disobbedienza del personale addetto al controllo e all'amministrazione delle informazioni, nonché al danneggiamento o alla manomissione delle attrezzature e/o delle connessioni.

4.5 Rischi di trattamento non conforme alle finalità della raccolta

I trattamenti non consentiti riguardano la possibilità che vengano effettuati trattamenti per cui l'interessato ha negato il necessario consenso previsto dalla legge oppure per i quali non è stata formalizzata la notificazione al Garante per la Protezione dei Dati Personali.

Tale rischio può presentarsi anche in relazione alla possibilità di effettuare trattamenti non conformi alle finalità della raccolta dei dati personali (obblighi contrattuali o pre-contrattuali, norme di legge o regolamenti, informative commerciali, ecc.).

4.6 Contromisure adottate

Per fronteggiare i rischi sopra esposti, sono state adottate idonee misure di sicurezza logica sia sul sistema operativo sia sugli applicativi e di sicurezza fisica. Le misure di sicurezza sono indicate nelle sezioni che seguono.

Parte Seconda

Misure di sicurezza

5. Protezione delle aree e dei locali

5.1. Criteri generali

Le misure di sicurezza, relative alle aree ed ai locali in cui sono ubicati i sistemi informatici contenenti i dati tutelati dalla normativa, sono finalizzate a minimizzare il rischio di danneggiamento o sottrazione di dati attraverso specifiche procedure che prevedono:

- il controllo per l'accesso agli edifici ed ai locali interni;
- le misure di sicurezza fisica aggiuntive e specifiche per gli elaboratori, gli apparati di trasmissione dati e i supporti magnetici per la protezione da furti e da danni volontari e involontari.

5.2. Procedure di accesso agli edifici ed ai locali interni

L'accesso alla sede centrale dell'ISPO, sita a Firenze in Viale Volta 171, è presidiato da personale di portineria/accettazione durante l'orario lavorativo.

Al di fuori dell'orario di apertura al pubblico, nessun soggetto esterno è autorizzato ad entrare nei locali dell'ISPO (la porta viene chiusa a chiave.)

I visitatori occasionali possono accedere ai locali dell'Istituto, previa richiesta telefonica da parte del personale della portineria con l'interessato, che ne deve autorizzare l'ingresso.

Per quanto riguarda le altre sedi dell'ISPO sono in atto misure del tutto analoghe. Inoltre per la sede di San Salvi e di Villa Le Rose è presente un sistema di anti intrusione.

5.3. Procedure di accesso alle sale macchine e apparati di controllo ambientale

I server della rete dell'ISPO della sede di Viale Volta 171 di Firenze sono ubicati in locali tecnici dedicati, il cui accesso è regolato da un dispositivo elettrico. L'accesso ai locali è riservato esclusivamente al personale dell'Unità Operativa Sistemi Informativo – EDP, ai sistemisti della ditta incaricata della gestione Sala Macchine, al personale addetto alla manutenzione. La responsabilità della gestione degli accessi al locale è di competenza dei sistemi informativi.

La sala macchine si trova al piano rialzato dell'edificio.

In relazione alle particolari esigenze di sicurezza ed operatività dei dispositivi hardware contenuti nel locale, sono state predisposte particolari misure di controllo ambientale specifiche.

Per quanto riguarda la protezione da possibili incendi, è presente un sistema di rilevazione della presenza di fumi attraverso dei sensori e un impianto di spegnimento automatico.

È inoltre presente un impianto di condizionamento dell'aria, composto da tre condizionatori indipendenti, in grado di mantenere costante la necessaria temperatura all'interno di tutta l'area interessata.

Infine, in caso di assenza prolungata di energia elettrica, una serie di UPS consentono di alimentare i server per consentire lo spegnimento controllato degli stessi.. L'apertura delle porte è consentita tramite budge in possesso del personale dell'Unità Operativa Sistema Informativo – EDP e della ditta che ne cura la gestione. Il locale, infine, è fornito di pavimentazione galleggiante e di vetrate anti sfondamento. Nelle sedi periferiche non sono previsti sistemi informatici.

6. Misure per garantire l'integrità dei dati

6.1. Criteri generali

L'amministrazione della sicurezza logica segue i seguenti criteri generali:

- la creazione dei codici identificativi e delle password è gestita dall' Unità Operativa Sistema Informativo - EDP;
- in base alle figure professionali presenti nell'Istituto, vengono definiti i profili standard da assegnare agli utenti con le autorizzazioni necessarie all'espletamento delle rispettive mansioni definite per ruoli e competenze;
- la validità delle richieste di accesso ai dati è verificata automaticamente dal sistema stesso prima di consentire l'accesso ai dati, tramite un sistema di autenticazione costituito da user-id e password.

6.2. Sistema di autorizzazione degli utenti

La creazione e la disabilitazione di utenze viene svolta dall'Unità Operativa Sistemi Informativi su richiesta dei Direttori di Unità Operative o Responsabili di Uffici.

6.3. Sistema di autenticazione degli utenti

I sistemi di controllo degli accessi logici ai dati ed alle applicazioni verificano i seguenti criteri generali:

- ciascun utente viene univocamente definito all'interno dei sistemi informativi attraverso l'attribuzione di un codice identificativo (user-id) personale a cui è associata sempre una password;
- il codice identificativo è assegnato in modo permanente all'utente e non può essere assegnato ad altri utenti neanche in tempi successivi;
- il codice identificativo viene disabilitato qualora l'utente cessi il suo rapporto con l'Istituto o;
- ciascun utente dispone di un codice identificativo associato a una "password".

6.3.1. Autenticazione per l'accesso alla rete locale

La sicurezza logica sulla rete locale è gestita dal responsabile dei Sistemi Informativi. Il sistema è caratterizzato dai seguenti punti di controllo, oltre ai criteri generali precedentemente esposti:

- l'accesso alla rete locale avviene tramite identificazione dell'utente con codici identificativi e password;
- la password di rete viene conservata in forma crittografata all'interno di un archivio protetto in lettura dal sistema di *security*;
- le password di rete prevedono una lunghezza minima di otto caratteri e sono sottoposte a scadenza periodica.

Le policy sono valide per tutti gli utenti abilitati all'accesso alla rete aziendale.

L'amministratore del sistema, pur non essendo direttamente a conoscenza delle parole chiave utilizzate dagli utenti per l'accesso ai dati presenti in rete, ha a disposizione gli strumenti necessari per cancellare e sostituire la password di ogni utente dietro debita autorizzazione del responsabile del trattamento dei dati.

I Responsabili delle Unità Operative\Uffici sono in possesso delle password di accensione dei PC degli utenti della UO in busta chiusa.

6.3.2. Autenticazione per l'accesso agli applicativi

In generale, passato il primo livello di autenticazione previsto dalla rete locale, l'accesso ai singoli applicativi richiede un secondo livello di autenticazione costituito da un altro codice identificativo con relativa password. Le password per l'accesso alle procedure applicative prevedono una lunghezza minima di otto caratteri.

Le password sono sottoposte a scadenza mensile in modalità automatica.

Le restanti misure di sicurezza logica implementate sugli applicativi seguono quanto indicato nei criteri generali. Esiste un progetto di standardizzazione delle postazioni di lavoro.

6.4. Misure di prevenzione di intrusioni e azioni di programmi ostili

ISPO ha predisposto idonee misure di sicurezza per la protezione dell'integrità dei propri dati da rischi connessi a programmi pericolosi (virus) o connessi ad alterazioni volontarie o involontarie dei dati, adeguando le stesse a quanto previsto dall'allegato B del codice in materia di protezione dei dati personali.

Per quanto riguarda il rischio di intrusione ad opera di programmi ostili, esso viene minimizzato attraverso l'adozione di misure tecniche ed organizzative.

La misura tecnica di sicurezza adottata in merito consiste nell'utilizzo di software antivirus, installato su tutte le postazioni di lavoro (*server e client* in rete). Il Sistema acquisisce in continuo gli aggiornamenti e, in maniera automatica, aggiorna le postazioni di lavoro.

Le *policy* di sicurezza e di aggiornamento possono essere impostate e modificate solo dall'amministratore dei sistemi.

Un sistema di "*live protection*" garantisce la scansione di tutti i file aperti e modificati, residenti su unità di memoria di massa locali, allegati a messaggi di posta elettronica e scaricati da Internet.

In caso di rilevamento di virus il programma provvede in maniera trasparente a riparare il file virato eliminando il virus; laddove questo non sia possibile sposta il file in una zona di quarantena.

Il personale incaricato dovrà osservare le seguenti raccomandazioni:

- prima dell'utilizzo è buona regola verificare sempre con gli appositi programmi antivirus tutti i sistemi di trasferimento dati (es. floppy disk, CD, ecc.);
- esaminare il file impiegando i programmi antivirus disponibili; nel caso il file risulti infetto, rimuovere il virus o contattare i sistemi informativi;
- utilizzare sempre programmi originali con dichiarazioni da parte dei fornitori;
- se possibile, evitare di scaricare cartelle, file, disegni, fotografie, ecc. da Internet in quanto il rischio virus è sempre molto elevato;
- non aprire messaggi di posta elettronica e file allegati agli stessi pervenuti da mittenti sconosciuti o con oggetto riconducibile a possibili attacchi da virus.

6.5. Misure di prevenzione di accessi abusivi e vulnerabilità degli strumenti

Il crescente utilizzo di reti di telecomunicazioni locali risponde all'esigenza di migliorare l'efficacia e l'efficienza dei processi aziendali, ma nello stesso tempo espone i sistemi informativi e le informazioni trattate a molteplici attacchi di disponibilità, integrità e riservatezza. La sicurezza della rete deve principalmente garantire da un lato l'utilizzo della risorsa trasmissiva ai soli utenti autorizzati e nelle specifiche modalità abilitate, e dall'altro che i dati contenuti in una comunicazione non possano essere:

- divulgati o alterati nel momento appena precedente al loro invio ad un destinatario;
- intercettati quando sono trasmessi sui mezzi di trasmissione compromettendo la loro integrità e/o riservatezza;
- conosciuti da utenti non autorizzati quando giungono a destinazione.

Le misure di sicurezza della rete sono implementate mediante restrizioni dell'accesso alla rete stessa. La scelta delle misure di sicurezza, inclusi gli apparati e/o i software è di competenza dell'Unità Operativa Sistemi Informativi.

La comunicazione/trasmissione dei dati mediante posta elettronica avviene tramite il software OutLook Express di Microsoft.

Le connessioni fra le sedi sono costituite da linee HDSL con linee ISDN di *back-up.*

La connessione da e verso Internet ed e-mail è garantita da un *firewall* gestito dal ISPO. La connettività è erogata dalla società Telecom Italia che fornisce anche l'apparato fisico di *routing.*

In generale, tutti gli accessi verso la rete pubblica sono controllati da apparecchiature per filtrare il traffico, quali Proxy, Firewall e Router.

7. Misure per garantire il ripristino della disponibilità dei dati

7.1. Salvataggio dei dati

L'Unità Operativa Sistema Informativo - EDP ha l'obbligo di curare l'aggiornamento e l'esecuzione delle procedure di *back-up* dei dati sui sistemi centrali. I salvataggi sono giornalieri. Viene effettuato il salvataggio di tutti i dati tramite software che va in esecuzione notturna.

7.2. Procedure di ripristino dei dati

L'Unità Operativa Sistema Informativo - EDP ha l'obbligo di curare l'aggiornamento e l'esecuzione delle procedure di ripristino del servizio nelle situazioni di emergenza che si possono presentare nell'operatività quotidiana (guasti hardware, software di base e applicativo, ecc.).

8. Criteri per il trattamento di dati all'esterno della struttura

La gestione dei servizi affidati a soggetti terzi che contengono dati personali e/o sensibili devono rispettare le regole del presente DPSS. L'elenco dei fornitori esterni per la gestione di servizi vari contenenti tutte le indicazioni necessarie alla loro identificazione è depositato presso la Struttura Acquisizione Beni e Servizi di ISPO. Ai fini del presente DPSS i fornitori di cui all'elenco risultano nominati quali Responsabili esterni al trattamento dei dati.

8.1 Norme di sicurezza

Nelle lettere di nomina dei fornitori a Responsabili Esterni, si è provveduto, a elencare dettagliatamente i compiti ad essi assegnati, l'ambito di responsabilità e le regole di condotta da seguire.

8.1. Separazione delle responsabilità / attività di sicurezza

I fornitori sono stati debitamente nominati Responsabili Esterni del trattamento dei dati personali assegnati nell'espletamento delle rispettive mansioni, così come previsto dal D. Lgs. 30 giugno 2003, N. 196; tale incarico s'intende valido ed efficace per tutta la durata del rapporto negoziale sottoscritto con ISPO. Nelle lettere di nomina sono state specificatamente indicate le responsabilità nonché i compiti che devono essere eseguiti ed osservati dai fornitori.

8.2. Standard di sicurezza di tutti i servizio dati in *outsourcing*

Nel caso di trattamento di dati sensibili, il fornitore deve predisporre un documento che precisi le norme e le soluzioni di sicurezza adottate per il servizio fornito a ISPO. Tale documento non deve essere in contrasto con il DPSS redatto da ISPO e con quanto prescritto dal D. Lgs. 30 giugno 2003, N. 196, deve essere vincolante per *l'outsourcer*.

8.3. Isolamento della rete/LAN

Il fornitore deve garantire che, per la parte di rete/LAN di sua responsabilità, con un'opportuna definizione di domini, sia evitato il rischio che altri suoi clienti o personale non autorizzato accedano ai sistemi o ai dati di ISPO.

8.4. Controlli e *Audit*

ISPO, in qualità di Titolare del trattamento dei dati personali, ha la facoltà di effettuare o far effettuare, controlli e *audit* per verificare lo stato della sicurezza del servizio prestato dai fornitori. Come riferimento dovrà essere presa la normativa vigente in materia di trattamento dei dati personali, nonché ulteriori istruzioni impartite da ISPO e concordate con il Fornitore stesso.

9. Criteri per il trattamento dei dati sanitari

9.1. Misure di sicurezza per dati trattati in elenchi, registri o banche dati

Per il trattamento dei dati sanitari idonei a rilevare lo stato di salute contenuti in elenchi, registri e banche dati, sono state adottate le seguenti misure di sicurezza:

- Le banche dati informatizzate sono consultabili solo dal personale autorizzato;
- Sui campioni biologici non sono riportati dati personali che possono identificare direttamente o indirettamente l'individuo;
- I dati contenenti i risultati delle analisi sono su Data Set diversi rispetto a quelli delle anagrafiche;
- I dati genetici sono aggregati in forma anonima al fine di analisi statistiche;
- Il trasporto all'esterno dei campioni biologici o il trasferimento dei dati personali contenuti nelle cartelle cliniche, viene effettuato solo da personale e\o collaboratori autorizzati, in contenitori sigillati;
- Il trasferimento dei dati in formato elettronico avviene in modalità cifrata.

Parte Terza

Formazione
&
Verifiche

10. 1.Informazione e formazione

Al fine di rendere edotto il personale Responsabile e Incaricato del trattamento dei dati sui contenuti e sulle implicazioni del D. Lgs. n. 196 del 30 Giugno 2003, è stata definita un'attività informativa svolta tramite la pubblicazione nell'Intranet dell'Istituto una serie di informazioni in materia di privacy. In particolare, si possono quindi individuare:

- informazioni di carattere generale quali "l'impegno" che il Centro vuole assumersi nel proteggere la Privacy dei dipendenti, dei soggetti che si avvalgono delle prestazioni del Centro e di ogni società terza che collabora con il Centro;
- la "Policy" sulla privacy;
- l'organizzazione interna con espressa indicazione degli estremi del Titolare e dei Responsabili;
- i documenti di lavoro.

Nel 2003, il 19 giugno si è svolto un corso rivolto ai Responsabili : **"La normativa vigente in tema di riservateza dei dati personali"**

Nel 2004, il 26 aprile si è svolto l'incontro formativo, rivolto ai Responsabili e Incaricati, sia dipendenti che consulenti e collaboratori, **"Introduzione alla nuova normativa privacy e principali aspetti per il settore sanitario"**, con i seguenti contenuti:

- Le norme generali sulla riservatezza e le discipline integrative per il settore della Sanità:
  - Fonti e novità normative;
  - Le definizioni introduttive;
  - Il Trattamento dei dati; il trattamento effettuato dagli Enti Pubblici;
  - La comunicazione dei dati personali e sensibili; precisazioni per gli Enti Pubblici e Sanitari;
  - Le figure individuate dalla legge: il Titolare, il Responsabile e l'Incaricato;
  - Adempimenti di legge: l'informativa e il consenso; precisazioni del Garante per il settore della Sanità;
  - Il Trattamento per scopi scientifici e statistici;
  - Cartelle cliniche;
- Le misure di sicurezza:
  - Gli standard minimi di sicurezza;
  - Novità legislative in tema di sicurezza;
  - Misure minime per il settore della Sanità;
  - Illustrazione del Documento Programmatico Sulla Sicurezza;
- Le sanzioni:
  - Amministrative, civili, penali;
  - Modalità dei controlli effettuati dall'Autorità Garante.

A tutto il personale che ha frequentato il corso di formazione, è stato rilasciato ampio spazio per formulare domande, anche con riferimento a casi pratici e specifici.

Nel 2005 il 14 giugno tutti i Responsabili Privacy, i direttori di U.O./Uffici, i responsabili dei vari servizi del ISPO, tutti gli Incaricati, hanno partecipato al Corso "**La Nuova Privacy e Le Professioni Medico-Sanitarie - Le problematiche Privacy al ISPO"**

1) NORME GENERALI SULLA RISERVATEZZA E LE DISCIPLINE INTEGRATIVE PER IL SETTORE DELLA SANITÀ

2) QUANTO E' STATO FATTO DAL ISPO IN MATERIA DI TUTELA DEI DATI PERSONALI

3) DISCUSSIONE APERTA SULLE PROBLEMATICHE PRIVACY AL ISPO :

- **comunicazione** del risultato degli esami agli utenti ISPO. In certi casi i medici di base vorrebbero/dovrebbero essere informati sull'esito degli esami: cosa dobbiamo fare? In quali casi è lecito comunicare il dato ?

- invio dei referti **per fax** fra strutture che collaborano con il ISPO

- comunicazione **telefonica** del referto

- referti in formato elettronico : parere sulla **conservazione della copia del referto cartaceo** se è disponibile nel computer di chi ha effettuato l'esame

- trattamento dati per programmi di ricerca condivisi **con strutture mediche europee o USA**: regole privacy.

- integrazione fra il concetto di **segreto professionale** e normativa in materia di privacy

- quali sono i trattamenti di dati che, essendo di rilevante interesse pubblico, possono essere effettuati senza consenso in ambito sanitario?

E' stato specifico obbligo dei Responsabili che hanno preso parte alla suddetta formazione, provvedere a rendere edotti dei contenuti del corso gli Incaricati della propria Unità Operativa\Ufficio, così da diffondere al massimo i principi fondamentali di comportamento in materia di protezione dei dati personali.

Nel 2006 il Corso Privacy rivolto a tutti i Responsabili e Incaricati si è svolto in due sessioni, in data **21 e 22 novembre** ed ha trattato i seguenti argomenti : **IL "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" E LA PUBBLICA AMMINISTRAZIONE. LE NUOVE REGOLE E I NUOVI ADEMPIMENTI**

1. Principi generali e definizioni.
2. Soggetti che effettuano il trattamento e loro responsabilità: titolare, responsabile e incaricato
3. Regole per il trattamento dei dati personali:
   - liceità dei dati personali
   - principio di necessità, pertinenza, non eccedenza;
   - comunicazione e diffusione
4. Lo schema tipo di regolamento per le Regioni e per le aziende sanitarie
5. Informativa agli interessati e consenso
6. Diritti dell'interessato e modalità di esercizio
7. Misure minime di sicurezza

8. Documento Programmatico per la sicurezza

DISCUSSIONE APERTA SULLE PROBLEMATICHE PRIVACY DELL' ISPO

NEL 2007 IL **5 giugno** il Corso Privacy rivolto a tutti i Responsabili e Incaricati ha riguardato

"Il trattamento dei dati sanitari e le regole per il trattamento dei dati per finalità di ricerca scientifica"

1. Trattamento dei dati personali in ambito sanitario
2. Informativa e consenso e relative modalità semplificate
3. Banche dati e registri
4. Ricerca scientifica
5. Dati genetici
6. Trattamento per scopi statistici

Di tutto il personale che ha frequentato i suddetti corsi di formazione è conservato il modulo di frequenza opportunamente controfirmato dal partecipante ed è stato rilasciato l'attestato di partecipazione e materiale informativo.

E' intenzione del Centro programmare la formazione anche per l'anno **2010** suddividendo il piano formativo in 3 diverse sessioni in ognuna delle quali verranno trattati argomenti specifici per il personale che svolge funzioni amministrative, sanitarie, epidemiologiche.

Inoltre, sono in fase di studio le modalità per inserire l'attività informativa sulle tematiche della privacy all'interno del percorso formativo per i dipendenti neo assunti.

Infine, il Centro avrà cura di aggiornare il modulo formativo con le necessarie integrazioni, in relazione all'evoluzione della normativa e alle indicazioni del Garante.

11. Verifiche periodiche

E' compito di Responsabili del trattamento assicurare le attività di revisione all'interno dell'Istituto, promuovendo ed effettuando i necessari controlli ispettivi sulle banche dati del ISPO, in collaborazione con le competenti Unità Operative\Uffici.

I Sistemi Informativi devono garantire il mantenimento di un adeguato livello di servizio, riservatezza e sicurezza del patrimonio informativo, per assicurare l'affidabilità, l'efficacia e l'efficienza delle procedure automatiche e di quant'altro connesso alla sicurezza ed al buon funzionamento delle strutture informatiche.

ALLEGATO "1"

Elenco dei trattamenti e dei responsabili per aree di attività

RIABILITAZIONE ONCOLOGICA

Settori di attività_
- Riabilitazione Oncologica

TRATTAMENTI	NOME APPLICAZIONE
In formato elettronico	
Follow-up riabilitazione	FWRI (*)
Servizio di riabilitazione fisica	PRIA (*) RIAB
Richiesta collaudo protesi	RIPR (*)
Gestione stomizzati	STOM (*)
Servizio psico/oncologia	PSIC (*)
Visite chirurgia plastica	PLAS (*)
Riabilitazione otorino	RIOT (*)

Tirocinanti
(*) anche cartaceo

In formato cartaceo

Cartelle cliniche relative alle prestazioni riabilitative

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 D. Lgs. 196/2003 è la **Dr.ssa Maria Grazia Muraca**

ATTIVITA' DI PREVENZIONE SECONDARIA SCREENING

Settori di attività:

- organizzazione e gestione per conto dell'Azienda Sanitaria di Firenze, o per altre Aziende Sanitarie che ne fanno richiesta tramite appositi rapporti convenzionali, le attività di screening cervico-vaginale, mammografico e colorettale
- gestione di un ambulatorio multidisciplinare di Genetica Oncologica per i carcinomi del colon-retto
- Centro di Riferimento Regionale per la prevenzione Oncologica
- coordinamento un'attività continua di consulenza professionale, formazione e assicurazione di qualità delle attività di screening oncologico, in collaborazione con le altre U.O. dell'Istituto
- ricerca (studi di valutazione di efficacia degli screening e di nuove metodologie e procedure di diagnosi precoce, anche in collaborazione con altri Istituti)
- didattica

TRATTAMENTI	**NOME APPLICAZIONE**
IN FORMATO ELETTRONICO	
Progetto controllo qualità del trattamento	SQTM(*)
Tumori mammella	
Genetica neoplasie colorettali	COGE (*)
Ambulatorio di dermatologia	DERM (*)
Visite gastroenterologiche	GAST (*)
Gestione consultori citologici	GECO
Screening mammografico	PSCR - SCRM (*)
Screening colon retto	SRET (*) - NSRE (*)
Esclusioni Screening	ESCL
Visite ginecologiche	VIGI (*)
File di risposte esami da consegnare (*)	
File di dati relativi a istologie e follow-up di patologie al seno	
File di visite oncologiche	
Follow-up utero	FWUT
Gestione Isteroscopie	PIST
Studio carcinoma prostatico	SPRO (*)
Gestione Esami MOC	MOCU
Visite medicina naturale	NATU
Esami del colon retto	RETT (*) RETX

Esami tiroide	PTIR
Casi e sospetti positivi utero	CSPU
Ecografie	ECOG
Archiviazione esami senologici	SENO
Studio sostenibilità della tecn. Digitale screening mamm.	ABRUZZO 1
Percorso screening oncologico RT	FLUSSO SCREENING
Progetto RIBES "rischi e benefici ecografia screening"	RIBES (*)
Valutazione coloscopia come test primario	SCORE 2 – SCORE 3
Anagrafe Istituto	ANSGRAFE01
Anagrafi Comuni provincia Firenze	PANA
Endoscopia Digestiva	EGAS
Visite Endocrinologia	ENDO
Prelievi sangue venoso	SAVE
Colloqui ginecologici	MENO
Prenotazioni ambulatoriali	AMBU

(*) **anche cartaceo**

IN FORMATO CARTACEO

Cartelle cliniche senologiche in attesa di archiviazione

Cartelle cliniche relative alle prestazioni riabilitative

Registri di appuntamenti per consulenza genetica

Referti di esami da consegnare

Copie di mammografie (se richieste dalla paziente) da consegnare

Raccolta dati relativi allo studio sulla mammografia digitale

Raccolta dati relativi allo studio sulle microcalcificazioni

Elenchi nominativi con esami clinici di donne afferenti allo screening cervico-vaginale

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Dr.ssa Carolina Cuzzoni.**

SENOLOGIA

Settori di attività:

- Senologia clinica (svolta in collaborazione con consulenti chirurghi dell'ASL di Firenze e dell'Azienda Ospedaliero-Universitaria Careggi), comprende :
    1. esame clinico
    2. indirizzo terapeutico
    3. servizio di follow-up
    4. consulenza di chirurgia ricostruttiva

- Senologia diagnostica-strumentale :
    1. esami mammografici
    2. esami ecografici
    3. prelievi con ago

Due archivi centralizzati, uno costituito da un juke-box di DVD-R e uno costituito da hard-disk, ricevono e memorizzano tutte le immagini digitali prodotte (mammogrammi, ecogrammi e stereo-mammogrammi)

- Ricerca :
    1. indirizzata prevalentemente alla elaborazione dei protocolli diagnostici e alla definizione delle procedure di follow-up

- Didattica

- Coordinamento del Servizio di accoglienza/portineria e accettazione prestazioni ambulatoriali

TRATTAMENTI	**NOME APPLICAZIONE**
IN FORMATO ELETTRONICO	
Procedura Follow up:	BASE
Follow-up seno:	FWSE
Consulenza genetica	GENE (*)
Refertazione esami senologici	NSEN (*) REAM_CURR
Esami senologici (orario agg.)	NSOA (*)
Rilev.dati tecnico di radiologia	RADM
Rilev.dati tecnico di radiologia (orario agg.)	RXOA
Server digitale di mammografia ed ecografia	
File di dati relativi allo studio Tamoxifen e studio HOT (*)	

(*) anche cartaceo

IN FORMATO CARTACEO

Cartelle cliniche senologiche in attesa di archiviazione

Referti di esami da consegnare

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è il **Dr. Beniamino BRANCATO**

CITOPATOLOGIA

Settori di attività:

- Citodiagnostica
    1. per lo screening cervico-vaginale dell'Azienda USL di Firenze
    2. per i servizi del CSPO e varie strutture ospedaliere fiorentine
- Gestione degli esami (accettazione, refertazione e archiviazione)
- Consulenze
- Didattica

TRATTAMENTI	**NOME APPLICAZIONE**
IN FORMATO ELETTRONICO	
Citologia mammaria	MAMM (*)
Citologia endometriale	PEND (*)
Citologia polmonare	POLM (*)
Citologia vaginale	PUTE (*)
Citologia urinaria	URIN (*)
File di dati relativi ad esami citologici eseguiti in regime di libera professione (*)	

(*) anche cartaceo

IN FORMATO CARTACEO

Copie di risposte istologiche di biopsie

Registri accettazione esami citologici

Cartelle cliniche di esami citologici in attesa di archiviazione

Registri di risposte positive citologia urinaria

Risposte di esami citologici da consegnare

Bolle di accompagnamento di esami citologici e istologici

Anagrafica partecipanti corsi e tirocini

BANCA BIOLOGICA COSTITUITA DA VETRINI IDENTIFICATI DA NUMERO PROGRESSIVO E/O DA CODICE ALFANUMERICO

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Dr.ssa Marzia Matucci**

CITOLOGIA ANALITICA E BIOMOLECOLARE

Settori di attività:

- Attività clinica :
    1. ricerca del virus HPV, determinazione di markers diagnostici e prognostici con metodiche immunologiche, immunocitochimiche,di biologia e genetica molecolare

- Screening :
    1. test per la ricerca del sangue occulto

- Ricerca (in due settori principali) :
    1. diagnostica oncologica molecolare
    2. fattori di rischio oncogeno

TRATTAMENTI **NOME APPLICAZIONE**

IN FORMATO ELETTRONICO

Hpv campioni interni 2006,2007,2008,2009

Hpv campioni SMA

NTCC campioni stoccati 29.4.2009

Campioni STUDIO PREGIO ISS

Colpo-FASE 1

Colpo- FASE 2

DNA Fecale

Elenco Donne Pre-Gio tutte

Esami –FASE 1

Esami – FASE 2

Gennp16 viapcio2005

GSK

Isto Cervice

Isto No Cervice

Italung Form- Bio Firenze

Italung Form- Bio Pisa

Italung Form-Bio Pistoia

NTCC "Fi Vt retesting"

NTCC "tipizzazioni"

Numero biopsia prostatectomia radicale PER DI LOLLO

Pio prostata campioni

PIO PROSTATA

PreGio 1

PreGio 2

Prospettico G.R.

RAS2000

RE-TESTING FIRENZE

Risultati RAS 2° invio

Self sampling

Server2Go

Studio SNP

Studio Olympus

Triage Viareggio, Empoli (sia archivio risposte che files con dati riassuntivi)

Italung studio marcatori TUTTO (16.12.2006)

Nuove tecnologie NUTE (*)

Studio HPV e Banca Biologica SHPV (*)

File di risposte esame in regime libera professione

File di risposte esami urgenti

File dati anagrafici di iscritti al GISCi (*)

File dati anagrafici di iscritti al GISCoR (*)

File campioni Banca Biologica (*)

(*) anche cartaceo

IN FORMATO CARTACEO

Cartelle cliniche di esami di laboratorio

Referti di esami da consegnare

Registri per accettazione esami di laboratorio

BANCA BIOLOGICA DI CAMPIONI IDENTIFICATI DA UN NUMERO PROGRESSIVO E/O DA CODICE ALFANUMERICO E/O DATI ANAGRAFICI PER DIAGNOSTICA MOLECOLARE ONCOLOGICA.

BANCA BIOLOGICA DI CAMPIONI IDENTIFICATI DA UN NUMERO PROGRESSIVO E/O CODICE ALFANUMERICO PER FATTORI DI RISCHIO ONCOGENO.

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Dr.ssa Tiziana RUBECA**

EPIDEMIOLOGIA CLINICO-DESCRITTIVA e VALUTAZIONE SCREENING

Settori di attività

- Epidemiologia descrittiva :
    1. Registro Tumori Toscano –Titolare del Trattamento è la Regione Toscana

- Attività di epidemiologia clinica (attività di ricerca e valutazione degli screening oncologici e dell'attività assistenziale):
    1. osservatorio nazionale per la prevenzione dei tumori femminili
    2. valutazione dei programmi di screening attivi nella Regione Toscana nell'ambito del Centro di Riferimento Regionale (CRR)
    3. attività di studio e ricerca nell'organizzazione dei programmi di screening mammografico, del cervico-carcinoma, del tumore colo-rettale
    4. valutazione di nuove tecnologie per la diagnosi precoce e per la qualità dell'assistenza in oncologia

- Attività didattica

TRATTAMENTI	**NOME APPLICAZIONE**
IN FORMATO ELETTRONICO	
Informazioni sanitarie relative alla patologia del paziente	CURE PALLIATIVE
Valutazione screening mammografico	
Valutazione screening cervice	
Valutazione screening colon retto	
Valutazione screening opportunistico mammografico	
Progetto Erotrial dati anamnestici, dati istologici e chirurgici relativi	EUROTRIAL
Registro Tumori	RTTS
Valutazione coloscopia come esame primario	SCORE 1 – Arezzo
Studio sorveglianza coloscopia nei familiari dei soggetti affetti da cancro colon-retto	CCR Familiarità Toscana
Referti istologici di Careggi, Prato, Empoli e Ponte a Niccheri per gli anni 1999 -2008-Dal 2004 anche altre AA.SS.LL. Dal 2005 anche AR e GR. –	REFERTI ISTOLOGICI
Ricoveri per patologia oncologica avvenuti nelle strutture sanitarie regionali per gli anni 1997-2006	RICOVERI

Screening della prostata (DRETRUS – PSA) con informazioni sulla eventuale causa di decesso	PROSTATA
Esenzioni per patologia tumorale maligna ASL di Firenze, Empoli e Prato (anni 1999-2005) 2003-2005 dati su tutta la Regione	ESENZIONI
Dati in forma anonima relativi alla casistica della mammella, Prostata, colon retto, polmone e melanoma	EUROCARE
Dati in forma anonima relativi al progetto EURELD	EURELD (*)
Dati in forma anonima relativi al progetto EOLO	EOLO (*)
Progetto staging degli anni 1995-1996	STAGING (*)
Progetto ITALUNG	ITALUNG
Progetto FRICAM "fattori di rischio carcinoma mammella"	FRICAM (*)
Soggetti iscritti al servizio sanitario nella Regione Toscana	ASSISTITI
Dati individuali non nominativi relativi a casi incidenti in Italia tumori del trofoblasto	REGISTRO NEOPLASIE GESTOTROFOBL. (*)
Archivi individuali nominativi e non di pazienti affetti da melanoma e altre patologie cutanee diagnosticate presso la Clinica Dermatologica dell'Università di Firenze	MELANOMA
Pazienti con lesione PIN diagnosticati presso CSPO	PIN
Software di cure palliative- dati individuali nominativi	QUA.LE.
Ricoveri ospedalieri	SDO
Dati in forma anonima relativi ai progetti specifici forniti da altri Enti	
Valutazione qualità – Rete onc. Toscana	GOVERNO CLINICO (*)

(*) anche cartaceo

IN FORMATO CARTACEO

Referti di anatomia patologica relativi al tumore dell'utero	TUMORI UTERINI
Referti di anatomia patologica-tumori del colon retto e schede di morte	SCORE 1
Dati relativi alle istologie della mammella negli anni 1990-1996 e schede di morte	
Questionari nominativi sulla valutazione dello screening mammografico	
Braccio toscano Studio implementazione dalle Liverpool Care Pathways	
Dati anagrafici nominativi più dati sanitari relativi al progetto sul polmone (Progetto Italung)	QUEST. POSTALI (*)

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è il **Dr. Marco Zappa**

EPIDEMIOLOGIA AMBIENTALE E OCCUPAZIONALE

Settori di attività

- Epidemiologia ambientale-occupazionale :
    1. studi analitici
    2. sorveglianza epidemiologica

- Consulenza (collabora con dipartimenti di prevenzione della ASL, agenzie regionali sanitarie, ecc…)

- Registro di Mortalità Regionale, Registro Mesoteliomi, Registro naso-sinusale, Registro ex art. 9 (Esposti Amianto) per i quali è Titolare del Trattamento la Regione Toscana

- Didattica

TRATTAMENTI	**NOME APPLICAZIONE**
IN FORMATO ELETTRONICO	
Studio sull'esposizione ambientale a benzene in un quartiere fiorentino	BENZENE FIRENZE (*)
Studio sulla morbosità e mortalità e classe socio-economica	CASE POPOLARI
Studio di citogenetica su addetti all'agricoltura	CITOGENETICA (*)
Questionario sull'abitudine al fumo di donne afferenti al CSPO	DONNE E FUMO (*)
Studio sui doppi tumori in pazienti affetti da Hodgkin	DOPPI TUMORI
Studio caso-controllo sulle neoplasie del sistema emolinfopoietico	EMOLINFOPIOETICO *
Studio sugli abitanti intorno a un impianto di smaltimento rifiuti	GIDA – Prato (*)
Studio sugli infortuni mortali in ambiente domestico	INFORTUNI MORTALI DOMESTICI (*)
Linkage dati SDO e INAIL	OCCAM
Studio su tumori polmonari	PIOMBINO
Indagine sulle donne afferenti all'ambulatorio di poliabortività e maternità dell'AO Careggi	POLIABORTIVITÀ CAREGGI (*)
Studio caso-controllo sulle leucemie e ras	RAS 1(*)
Studio sulla salute riproduttive delle dipendenti di aziende sanitarie	SALUTE RIPRODUTTIVA DONNA LAVORATRICE(*)
Studio caso-controllo sulle leucemie infantili	SETIL (*)
Studio sui disturbi respiratori infantili	SIDRIA (*)
Survey sulla salute delle donne	SURVEYVIGILI DONNE
Studio caso-controllo sui tumori rari	TUMORI RARI (*)
survey sull'esposizioni professionali nei calzaturifici	VALIDAZIONE ESPOSIZIONE CEE(*)

studio caso-controllo sul tumore alla vescica	VESCICA(*)
Registro Mortalità	PMOR
Registro Mesoteliomi	
Registro Naso-Sinusale	
Registro ex art. 9 (esposti amianto)	

Studi di coorte su possibili esposti a cancerogeni professionali:

Amiata (*)
Anic (*)
Baraclit (*)
Biblioteca Nazionale (*)
Borma (*)
Breda (*)
Cantieri Navali Massa (*)
Cappellifici
Comunale (*)
Cokeria(*)
Conciatori (*)
Cooperativa Tassisti fiorentini (*)
Coorte Pietra Serena
De Micheli (*)
Fervet (*)
Fibronit (*)
Fiori coorte e familiari (*)
Florovivaisti di Pistoia
Fissi (*)
Fitofarmaci Siena
Ginori (*)
Portuali Livorno
Rangoni (*)
Riparazioni FFSS (*)
Saint Gobain (*)
Saivo (*)
Saline Volterra(*)
Santa Lucia
Silicotici 1946-79
Signani (*)
Siri (*)
Toscana Tubi (*)

Wittenoon Toscana

(*) anche cartaceo

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Dr.ssa Elisabetta Chellini**

EPIDEMIOLOGIA MOLECOLARE E NUTRIZIONALE

Settori di attività

- Epidemiologia molecolare e nutrizionale
- Epidemiologia genetica
- Prevenzione dei tumori
- Sviluppo e gestione di banche biologiche e di banche dati alimentari
- Sviluppo e gestione di programmi per la raccolta e l'analisi di informazioni sulle abitudini dietetiche
- Didattica

TRATTAMENTI

IN FORMATO ELETTRONICO

Banche dati UO Epidemiologia Molecolare e Nutrizionale

Studio EPIC – Firenze

Studio determinanti pattern mammografico e tumore della mammella

Studio di coorte malattie infiammatorie croniche intestinali

Studio epidemiologia molecolare mammella maschile

Studio epidemiologia molecolare mammella femminile familiare

Studio epidemiologia molecolare tumore stomaco

Studio epidemiologia molecolare tumore familiare prostata

Studio epidemiologia molecolare su melanoma e altri tumori cutanei

Studio epidemiologia molecolare tumore mammella femminile

Trial olio di oliva

Studio di intervento randomizzato DAMA

Studio epidemiologia molecolare sarcomi ossei e dei tessuti molli

Studio di coorte soggetti con biopsia gastrica

Studio linfomi gastrici

Studio Casentino

Studio caso-controllo multicentrico italiano su tumore gastrico

Studio di incidenza e studio caso-controllo sui linfomi cutanei

Studio determinanti della infezione da Helicobacter pylori

Studio Loiano

Studio Inchianti

Studio caso-controllo tumore laringe

Studio di coorte su soggetti obesi

Studio sulle complicanze dell'ulcera peptica

Studio tumori incidentali prostata

Studio di coorte IBD Palermo

Studio casistica di tumori del retto

Studio sui determinanti dietetici e molecolari del tumore colorettale (

(Progetto AIRC Regionale)

Progetto "Diagnosi precoce del tumore gastrico nell'area del Mugello"

Studio "Epidemiologia molecolare del tumore del colon"

Studio GIVIO "Effetti di un diverso protocollo di follow-up in una coorte di pazienti affetti da tumore della mammella"

Studio randomizzato di un vino dealcolizzato ricco in polifenoli antiossidanti in volontari sani: effetti sullo stress ossidativo cellulare e sull'espressione genica

Studio sul recettore CXCR3-B e necrosi tumorale nel carcinoma renale

Abitudini dietetiche e di stile di vita di soggetti coinvolti in uno studio caso controllo sul tumore della prostata (studio condotto dal CPO-Torino)

Abitudini dietetiche e di stile di vita di soggetti coinvolti in uno studio caso controllo sul tumore dell'endometrio (studio condotto dal ISI-Torino)

Studio di validazione del questionario EPIC sulla attività fisica e di altri due questionari riguardanti l'attività fisica (IPAQ usato a livello europeo e RPAQ Cambridge).

Studio di mortalità e morbidità di una coorte di sportivi afferenti al centro di medicina dello sport di Pisa

Studio Trasversale Viareggio

Mortalità a lungo termine in una casistica di soggetti con alcoldipendenza

Solo numero identificativo Studio EPIC – Italia

Solo numero identificativo Studio EPIC – Europa

Solo numero identificativo Studio sui determinanti dei sintomi di reflusso gastroesofageo:

Solo numero identificativo Studio sul tumore della prostata

Solo numero identificativo Studio su rigidità arteriosa e attività fisica in soggetti normo e ipertesi

Solo numero identificativo Inchiesta su abitudini alimentari e stile vita nell'ambito dello studio intervento di promozione della salute nella azienda Eaton (Massa)

Solo numero identificativo Ruolo della radioterapia in una serie di tumori del polmone "non a piccole cellule"

Solo numero identificativo Ruolo di alcuni marcatori sierici, quali IGF-I and IGF-BP3, nella diagnosi di deficit di GH nei bambini di bassa statura

Solo numero identificativo Sviluppo di tumore della mammella nel follow-up di una casistica di M. Hodgkin

Solo numero identificativo Effetto di diversi protocolli di chemioterapia nel trattamento del tumore della mammella

Solo numero identificativo Effetto della radioterapia in un serie di adenoma ipofisario

Solo numero identificativo Effetto della radioterapia in un serie di tumori dell'endometrio

La UO legge tramite lettore ottico ed esegue controlli di qualità su files con identificativo (non nominativo) per progetti che utilizzano il questionario alimentare EPIC, limitatamente ai dati raccolti con quel questionario. I files e il materiale cartaceo relativo vengono conservati solo per il tempo necessario a tale attività.

BANCA BIOLOGICA DI CAMPIONI IDENTIFICATI DA UN NUMERO PROGRESSIVO E/O DA CODICE ALFA NUMERICO

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Dr.ssa Giovanna MASALA**

AREA TECNICA SANITARIA

Il personale tecnico svolge varie attività, tra le quali in particolare:

1. allestimento di campioni biologici ed esecuzione di attività di laboratorio, di radiologia, ambulatoriali, cliniche, trattamenti riabilitativi, ecc…
2. attività didattica

TRATTAMENTI

IN FORMATO ELETTRONICO

Gestione dati anagrafici di partecipanti a corsi di formazione per tecnici di radiologia

Gestione archivio su supporto magnetico di dati anagrafici ed immagini radiografiche per procedura stereotassica

Gestione consolle per refertazione di esami di mammografie di screening

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Sig.ra Elisabetta GENTILE**

S.C. BIOSTATISTICA

Settori di attività

- Ricerca valutativa (effettuata in relazione a studi epidemiologici svolti dalle varie Unità Operative dell'Istituto, secondo un programma di lavoro coordinato)
    1. analisi statistica dei dati di genomica funzionale
    2. disegno ed analisi degli studi clinici controllati e osservazionali
    3. statistica spaziale e rappresentazioni cartografiche, analisi delle aggregazioni spaziali di casi di malattia
    4. disegno e conduzione di meta-analisi

TRATTAMENTI	**NOME APPLICAZIONE**
Casistica relativa al censimento popolazione 1991 con i dati relativi al Registro Tumori per gli anni: 1981-2001 Livorno 1991-2001 Firenze 2001 Prato (ISPO partecipa allo Studio come Istituto compartecipante, la titolarità è di Regione Toscana)	ST. LONGITUDINALE

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è il **Prof. .Annibale BIGGERI**

S.S. FORMAZIONE E COMUNICAZIONE

Settori di attività

1. costituisce il riferimento amministrativo per le attività di formazione esterna ed aggiornamento del personale

TRATTAMENTI

In formato elettronico

Anagrafica di giornalisti)*)

Anagrafica di partecipanti a corsi di formazione (*)

Curriculum formativi di dipendenti, collaboratori, docenti dei corsi (*)

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Dr.ssa Carolina Cuzzoni**

S.C. STAFF TECNICO AMMINISTRATIVO

Gestisce la propria attività in sinergia con l'Azienda Sanitaria di Firenze

1. Provvede al supporto amministrativo gestionale delle strutture scientifiche e sanitarie dell'Istituto
2. Costituisce il nucleo operativo che affianca strettamente la Direzione Scientifica e la Direzione Sanitaria
3. Provvede, in collaborazione con le strutture sanitarie, alla gestione dei finanziamenti finalizzati all'attività di ricerca in regime convenzionale.
4. Cura la stipula e gestione delle convenzioni passive con altre Aziende del S.S.N. e con privati per lo svolgimento di prestazioni sanitarie, di consulenza, ecc.
5. Predispone gli atti relativi allo svolgimento di frequenze volontarie e tirocini post - laurea, ecc. da parte di personale non dipendente

TRATTAMENTI

IN FORMATO ELETTRONICO

Anagrafica di personalità di istituzioni scientifiche e non, sia della Regione Toscana che del territorio nazionale ed europeo (*)

Dati personali relativi a pratiche legali e convenzioni

Dati anagrafici di Direttori Generali di AA.SS.LL, AA.OO., Enti pubblici e privati, Istituzioni, Professionisti esterni

Dati giudiziari (pratiche legali)

Indirizzari di utenti per inviare risposte e chiarimenti di eventuali reclami (*)

Accettazione ACCE

Libera Professione

Protocollo (*)

(*) anche cartaceo

IN FORMATO CARTACEO

Schede con dati personali e/o sensibili pervenuti all'URP per segnalazioni, suggerimenti e reclami in relazione alla qualità delle prestazioni e servizi del CSPO

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è **il Dr. Giorgio Nencioni**

CONTABILITA' GENERALE E CONTROLLO DI GESTIONE

Gestisce la propria attività in sinergia con l'Azienda Sanitaria di Firenze

1. Svolge attività di gestione economico-finanziaria ivi inclusa l'attività di controllo economico sulla gestione complessiva dell'Istituto utilizzando gli strumenti della contabilità generale ed analitica
2. Gestisce la cassa economale

TRATTAMENTI **NOME APPLICAZIONE**

IN FORMATO ELETTRONICO

Procedura contabilità generale ed analitica (dati relativi a fornitori,clienti e debitori)

(*) anche cartaceo

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è la **Dr.ssa Cristina Gheri.**

ACQUISIZIONE BENI E SERVIZI

Provvede a garantire l'approvvigionamento dei beni e servizi necessari per il funzionamento dell'Istituto avvalendosi di ESTAV-Centro

TRATTAMENTI

IN FORMATO ELETTRONICO E CATRACEO

Dati anagrafici di fornitori per l'acquisto di beni di consumo e durevoli

Dati relativi a contratti di leasing e canoni di noleggio

Responsabile dei suddetti trattamenti ai sensi dell'art. 29 del D.Lgs. 196/2003 è il **Dr. Giorgio Nencioni**

Strutture aziendali da partecipare :

Direzione Sanitaria
Referente Privacy ISPO
UU.OO. Istituto