ISTITUTO NAZIONALE TUMORI
I.R.C.C.S. "FONDAZIONE G. PASCALE"

Documento Programmatico sulla Sicurezza

Direttore Generale
Dr. Tonino Pedicini

AGGIORNAMENTO

Il presente documento è predisposto in attuazione del punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (Decreto legislativo 30 giugno 2003, n. 196)

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

INDICE DEL DOCUMENTO

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

1. SCOPO.

Il presente documento costituisce l'aggiornamento del Documento Programmatico sulla Sicurezza, adottato con Deliberazione n. 853 del 22/11/2005.
Esso ha lo scopo di delineare il quadro delle misure di sicurezza organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato dall'ISTITUTO NAZIONALE TUMORI I.R.C.C.S. FONDAZIONE PASCALE di Napoli.
Conformemente a quanto prescrive la regola 19 del Disciplinare tecnico, allegato sub b) al D.Lgs. n. 196/2003, nel presente documento si forniscono idonee informazioni riguardanti:
1. l'elenco dei trattamenti di dati personali (punto 19.1 del disciplinare), mediante:
   - la individuazione dei tipi di dati personali trattati;
   - la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
   - la elaborazione della mappa dei trattamenti effettuati, che si ottiene incrociando le coordinate dei due punti precedenti;
2. la distribuzione dei compiti e delle responsabilità, nell'ambito delle strutture preposte al trattamento dei dati (analisi del cd. mansionario privacy: punto 19.2 del disciplinare) e la previsione di interventi formativi dei Responsabili e degli Incaricati del trattamento (punto 19.6 del disciplinare);
3. l'analisi dei rischi che incombono sui dati (punto 19.3 del disciplinare);
4. le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati (punto 19.4 del disciplinare);
5. i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento (punto 19.5 del disciplinare);
6. i criteri da applicare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno (punto 19.7 del disciplinare);
7. le procedure da seguire per il controllo sullo stato della sicurezza.

2. ORGANIZZAZIONE DELL'AZIENDA.

L'ISTITUTO NAZIONALE TUMORI I.R.C.C.S. FONDAZIONE PASCALE è un'Azienda pubblica che eroga servizi sanitari.
Assolve il compito istituzionale di tutela e promozione della salute della collettività nell'ambito delle indicazioni nazionali e regionali, mediante la predisposizione ed attuazione di obiettivi volti al miglioramento continuo dell'assistenza ed equità delle prestazioni.

L"ISTITUTO NAZIONALE TUMORI I.R.C.C.S. FONDAZIONE PASCALE ha sede in Napoli in via Mariano Semmola.

Sedi operative :
- Via Mariano Semmola, Napoli (sede principale);
- Centro Ricerche Oncologiche Mercogliano (C.R.O.M.), via Ammiraglio Bianco, Mercogliano (AV);

I principali servizi erogati sono così ripartiti:
·SERVIZI AREA SANITARIA;
·SERVIZI AREA AMMINISTRATIVA.

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

3. TIPOLOGIA DI DATI TRATTATI

Da un punto di vista assolutamente generale le attività istituzionali di un I.R.C.C.S. si possono dividere in Amministrative e Sanitarie. Ambedue comportano flussi informativi interni ed esterni all'Azienda e coinvolgono collaboratori che possono essere o meno alle dirette dipendenze dell'Azienda.
Le modalità con cui i dati personali e sensibili sono trattati possono essere le più disparate e prevedono sia sistemi di elaborazione automatica che utilizzi di tipo cartaceo (documenti autografi, stampe di documenti elettronici, modulistica, fax, fotocopie, etc) o verbale (radio, conversazioni, lezioni, etc).
In questo paragrafo viene data una panoramica delle informazioni trattate, con particolare attenzione a quelle che sono state oggetto di notifica al Garante.

3.1 CATEGORIA E NATURA DEI DATI TRATTATI.

• INFORMAZIONI ANAGRAFICHE : elementi d'identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato e di lavoro, Codice Fiscale, num. di libretto sanitario, num. di telefono, di telefax, indirizzo di posta elettronica, numero carta d'identità, passaporto, patente di guida, n. posizione previdenziale e assistenziale, dati fisici quali altezza e peso);

• STATO DI SALUTE**:** questo tipo di informazione è relativa sia agli assistiti che al personale dipendente (certificati medici per assenza a causa di malattie). In particolare i dati sanitari riguardano : diagnosi, prognosi, cure, prestazioni, referti, interventi, analisi, analisi strumentali.

• DATI GENETICI: in carico al centro trasfusionale, ematologia, nefrologia;

• DATI RELATIVI ALLA FAMIGLIA e a situazioni personali (stato civile, minori a carico, consanguinei, altri appartenenti al nucleo famigliare);

• ISTRUZIONI E CULTURA (pianificazione degli iter formativi interni, curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audio-visivo, ecc. - titoli di studio);

• LAVORO: Queste informazioni sono relative prevalentemente ai dipendenti e riguardano: occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione personale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae o lavorativo, competenze professionali, retribuzione, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente;

• ADESIONE A SINDACATI od organizzazioni a carattere sindacale; relativi a dipendenti iscritti a sindacati cui l'Azienda versa la quota associativa.

• CONVINZIONI RELIGIOSE, adesioni ad organizzazioni a carattere religioso; (assistenza religiosa ai ricoverati, diete alimentari derivanti da particolari pratiche e convinzioni religiose,….)

• DATI CONTABILI, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni, identificativi finanziari, solvibilità, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi, dati assicurativi, dati previdenziali);

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

- Informazioni di tipo GIUDIZIARIO (sulla posizione nel casellario giudiziale richieste ai dipendenti all'atto dell'assunzione, contenziosi sia penali che civili con soggetti interni ed esterni all'Azienda).

3.2 SOGGETTI CUI SI RIFERISCONO I DATI .

Le macro-categorie di soggetti fisici e giuridici interessati a cui si riferiscono i dati personali e sensibili trattati dall'Amministrazione sono :

• CITTADINO UTENTE delle prestazioni sanitarie (vengono fornite prestazioni a tutti i cittadini italiani e stranieri che si presentino presso le sedi dell'Istituto Pascale).
• PERSONALE DIPENDENTE;
• PERSONALE NON DIPENDENTE (retribuito o meno) che collabora con l'Amministrazione o con società, enti, associazioni, etc. che offrono prestazioni all'Istituto Pascale:

- LAVORATORI AUTONOMI e LIBERI PROFESSIONISTI;
- MEDICI VOLONTARI;
- CONSULENTI;
- SPECIALIZZANDI;
- ADERENTI AD ASSOCIAZIONI POLITICHE, RELIGIOSE O SINDACALI;
- SOGGETTI OD ORGANISMI PUBBLICI;
- CANDIDATI da considerare per l'instaurazione di un rapporto di lavoro;
- FREQUENTATORI;
- FAMILIARI E AFFINI dell'interessato.

3.3 FINALITA' DEI TRATTAMENTI.

Le finalità del trattamento sono riconducibili alle seguenti macro-categorie :

• Finalità connesse al settore sanitario;
• Finalità amministrative e contabili;
• Finalità di carattere sociale;
• Finalità connesse alla gestione del personale interno e dei collaboratori esterni;
• Finalità connesse alla ricerca scientifico-sanitaria;
• Finalità connesse alla formazione specialistica.

3.4 DATI TRATTATI

I dati trattati dal Titolare, sono stati suddivisi in relazione alla loro natura e alle macroaree di riferimento dove avviene il loro trattamento (ovvero area sanitaria o amministrativa).
Per ognuna delle suddette tipologie di dati, sono stati individuati, inoltre, i soggetti cui tali dati si riferiscono.

Dati diversi da quelli sensibili e giudiziari (dati comuni)

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

Area sanitaria

- nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro, indirizzo di posta elettronica, numero di telefono e di fax, posizione rispetto agli obblighi militari, dati fisici);
- codice fiscale ed altri numeri di identificazione personale (carte sanitarie, numero carta di identità, passaporto, patente di guida, numero di posizione prevenzione o assistenziale);
- dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei) altri appartenenti al nucleo familiare;
- istruzione e cultura (curriculum di studi e accademico, titoli di studio, pubblicazioni);
- dati concernenti l'attività lavorativa (occupazione attuale e dati sulle occupazioni precedenti, informazioni sul reclutamento/tirocinio/formazione professionale, competenze professionali, cariche pubbliche rivestite, retribuzioni, assegni, integrazioni salariali e trattenute, dati sulla gestione/valutazione delle attività lavorative);
- attività economiche, commerciali, finanziarie e assicurative ovvero dati relativi all'affidabilità o puntualità nei pagamenti, alla solvibilità economica, all'adempimento di obbligazioni, informazioni commerciali, (solo per collaboratori esterni);
- beni, proprietà, possessi (solo per collaboratori esterni);

relativi alle seguenti categorie di soggetti:

- pazienti/assistiti anche deceduti (esclusa la categoria dei dati concernenti l'istruzione/cultura e l'attività lavorativa);
- personale sanitario (consulenti, dipendenti, figure sanitarie, figure di comparto, operatori tecnici di reparto, ausiliari specializzati e altro personale) ed ai candidati a diventarlo;
- collaboratori esterni, ovvero cooperative e ditte fornitrici di beni e servizi ed ai candidati a diventarlo.

Area amministrativa

- nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro, indirizzo di posta elettronica, numero di telefono e di fax, posizione rispetto agli obblighi militari, dati fisici);
- codice fiscale ed altri numeri di identificazione personale (carte sanitarie, numero carta di identità, passaporto, patente di guida, numero di posizione prevenzione o assistenziale);
- dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare);
- istruzione e cultura (curriculum di studi e accademico, titoli di studio, pubblicazioni);
- dati concernenti l'attività lavorativa (occupazione attuale e dati sulle occupazioni precedenti, informazioni sul reclutamento/tirocinio/formazione professionale, competenze professionali, cariche pubbliche rivestite, retribuzioni, assegni, integrazioni salariali e trattenute, dati sulla gestione/valutazione delle attività lavorative);
- attività economiche, commerciali, finanziarie e assicurative ovvero dati relativi all'affidabilità o puntualità nei pagamenti, alla solvibilità economica, all'adempimento di obbligazioni, informazioni commerciali, (solo per collaboratori esterni);
- beni, proprietà, possessi (solo per collaboratori esterni);

relativi alle seguenti categorie di soggetti:

- personale dipendente tecnico-amministrativo ed ai candidati a diventarlo;
- personale sanitario (consulenti, dipendenti,, figure sanitarie, figure di comparto, operatori tecnici di reparto, ausiliari specializzati) ed ai candidati a diventarlo;

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

- collaboratori esterni, ovvero cooperative e ditte fornitrici di beni e servizi, ed ai candidati a diventarlo.

Dati sensibili

Area sanitaria
- dati idonei a rivelare le origini razziali o etniche;
- dati idonei a rivelare le convinzioni religiose, adesioni a organizzazioni a carattere religioso;
- dati idonei a rivelare lo stato di salute, in particolare:
  - dati idonei a rivelare l'appartenenza a categorie protette;
  - dati idonei a rivelare la vita sessuale;
  - dati idonei a rivelare lo stato di inabilità;
  - dati idonei a rivelare sieropositività;
  - dati idonei a rivelare malattie infettive e diffusive;
  - dati idonei a rivelare malattie mentali;
  - dati idonei a rivelare stato di salute;
  - dati relativi a indagini epidemiologiche;
  - dati relativi a prescrizioni farmaceutiche e cliniche;
  - dati relativi ad esiti diagnostici e programmi terapeutici;
  - dati relativi all'utilizzo di particolari ausili protesici;
  - dati relativi alla prenotazione di esami clinici e visite specialistiche;
  - dati idonei a rilevare HIV conclamato;
  - dati inerenti a caratteristiche o idoneità psichiche;

relativi alle seguenti categorie di soggetti:
- pazienti/assistiti (anche deceduti);
- personale dipendente tecnico-amministrativo ed ai candidati a diventarlo;
- personale sanitario (consulenti, dipendenti, figure sanitarie, figure di comparto, operatori tecnici di reparto, ausiliari specializzati.) ed ai candidati a diventarlo.

In particolare per il personale dipendente (sanitario e tecnico-amministrativo), relativamente alla categoria dei dati idonei a rivelare lo stato di salute, sono escluse alcune categorie di informazioni non di pertinenza.

Area amministrativa
- dati idonei a rilevare la adesione a sindacati o organizzazioni a carattere sindacale;
- dati idonei a rivelare la vita sessuale (stato di gravidanza);
- dati idonei a rivelare lo stato di salute, in particolare:
  - dati idonei a rivelare l'appartenenza a categorie protette;
  - dati idonei a rivelare lo stato di inabilità;
  - dati idonei a rivelare stato di salute;
  - dati relativi a prescrizioni farmaceutiche e cliniche;
  - dati relativi ad esiti diagnostici e programmi terapeutici;
  - dati relativi all'utilizzo di particolari ausili protesici;
  - dati relativi alla prenotazione di esami clinici e visite specialistiche;

relativi alle seguenti categorie di soggetti:

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

- personale dipendente tecnico-amministrativo ed ai candidati a diventarlo;
- personale sanitario (consulenti, dipendenti, figure sanitarie, figure di comparto, operatori tecnici di reparto, ausiliari specializzati) ed ai candidati a diventarlo.

Dati genetici

Area sanitaria
- dati idonei a rivelare patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali;
- dati idonei a rivelare la gravità o il decorso del quadro clinico delle patologie genetiche;
- dati idonei a identificare malattie ereditarie;
- dati relativi alle malformazioni congenite la cui causa non e' nota;
- dati idonei ad accertare maternità o paternità;
- dati relativi a indagini epidemiologiche;
- dati relativi a indagini sulla popolazione;
- dati relativi alla procreazione;
- dati tratti da studi di relazione tra patrimonio genetico e fattori di rischio relativi a pazienti/assistiti.

Area amministrativa
Nessun dato trattato

Dati giudiziari

Area sanitaria
- dati relativi a comportamenti illeciti o fraudolenti;
- dati relativi ad altri provvedimenti o procedimenti giudiziari;
- dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o contabili relativi alle seguenti categorie di soggetti:
- pazienti/assistiti

Area amministrativa
- dati relativi a comportamenti illeciti o fraudolenti;
- dati relativi ad altri provvedimenti o procedimenti giudiziari;
- dati relativi ad altri provvedimenti o procedimenti sanzionatori, disciplinari, amministrativi o Contabili;

relativi alle seguenti categorie di soggetti:
- personale dipendente tecnico-amministrativo ed ai candidati a diventarlo;
- personale sanitario (consulenti, dipendenti, figure sanitarie, figure di comparto, operatori tecnici di reparto, ausiliari specializzati) ed ai candidati a diventarlo;
- collaboratori esterni (cooperative e ditte fornitrici di beni e servizi) ed ai candidati a diventarlo.

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

4. SEDI DEL TRATTAMENTO

Il trattamento dei dati è svolto sia nella sede principale dell'Istituto, ubicata in via Mariano Semmola in Napoli, che nella sede del C.R.O.M. di Mercogliano (AV), alla via Ammiraglio Bianco.

5. STRUMENTI UTILIZZATI PER IL TRATTAMENTO

Le operazioni di trattamento dei dati indicate dall'art. 4 D.Lgs. n. 196/03 riguardano i trattamenti effettuati con l'ausilio di strumenti elettronici e senza l'ausilio di strumenti elettronici (trattamento su supporto cartaceo).
L'Azienda effettua trattamenti con e senza l'ausilio di strumenti elettronici.

5.1 Documenti cartacei.

I supporti cartacei contenenti i dati personali, vengono archiviati, una volta terminato il ciclo lavorativo, in locali, schedari, armadi, cassetti dotati di chiave.

Il complesso degli atti, dei documenti e dei dati prodotti o acquisiti dal soggetto produttore nell'esercizio delle sue funzioni è definito come archivio.
Gli archivi cartacei si distinguono in:

- archivi correnti (insieme dei documenti correnti): tenuti dai singoli Incaricati e/o Responsabili negli uffici e nelle aree operative o tenuti dal personale nei reparti di cura;
- archivi di deposito (insieme dei documenti semi-attivi): archivi ad accesso ristretto presenti in alcune unità operative e archivi centralizzati, mantenuti a cura del relativo Responsabile o Incaricato;
- archivi storici (insieme dei documenti storici): archivi mantenuti per motivi storici o per esigenze di legge.

Il trattamento di dati effettuato "manualmente" è disciplinato espressamente dall'art. 35 D.Lgs. n. 196/03 e dall'allegato B (disciplinare tecnico).

5.2. Trattamento con l'ausilio di strumenti elettronici (elaboratori in rete privata).

L'Azienda dispone di una rete privata (o rete LAN) cui sono allacciati tutti gli elementi hardware/elettronici nell'ambito della stessa struttura, sulla quale possono viaggiare i dati elettronici di proprietà.
Tutte le unita organizzative, sono collegate direttamente, alla sede legale dell'Azienda, conseguentemente, tutti i dati elettronici trattati presso le unità organizzative alla fine del ciclo di trattamento, risiedono fisicamente in apposite banche-dati elettroniche (specifiche per i vari sistemi informatici impiegati).
Tutti gli utenti perciò, attraverso i vari PC collegati e distribuiti nell'ambito dell'intera struttura (postazioni fisse-client) e dopo il superamento di apposite procedure di autenticazione ed autorizzazione possono accedere ai dati contenuti in una delle suddette banche dati, utilizzando lo specifico sistema informatico di riferimento
Tutti gli utenti autorizzati, attraverso i vari PC collegati e distribuiti nell'ambito dell'intera Azienda
(postazioni fisse-client), possono collegarsi alla rete pubblica per l'accesso, attraverso appositi sistemi informatici, ad alcune banche dati elettroniche messe a disposizione dalla Regione

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

ove autorizzati inoltre, gli utenti possono accedere anche ad Internet, attraverso i vari PC collegati e distribuiti nell'ambito dell'intera Azienda.
Attualmente, presso le UU.OO e gli uffici amministrativi vengono impiegati PC per le attività istituzionali assegnate.

Locali CED.

Il sistema di lavoro della struttura avviene con elaborazione in rete privata/pubblica.
Si dispone di una rete, realizzata mediante collegamenti via cavo e VPN costituita .

6. MAPPA DEI TRATTAMENTI EFFETTUATI.

Nel corso dell'anno 2011 l'Azienda ha effettuato il censimento della tipologia dei possibili trattamenti effettuati sui dati dal personale dell'Istituto nell'ambito delle proprie competenze e delle relative strutture di appartenenza preposte al trattamento dei dati .
Tutti i documenti sono custoditi presso l'Ufficio Privacy incardinato presso la U.O.C. Affari Legali.

Elenco trattamenti: informazioni essenziali

VEDI ALLEGATI A e D

7. MANSIONARIO PRIVACY.

I ruoli, incarichi e competenze delle varie figure coinvolte sono dettagliatamente indicati nel Regolamento aziendale Privacy adottato con Delibera n. 628 del 30/06/2011.

Il Titolare del trattamento dei dati è l'Istituto Nazionale per lo Studio e la Cura dei Tumori - Fondazione Giovanni Pascale, nella persona del suo legale rappresentante il Direttore Generale.

Il Referente aziendale privacy ed il Consulente aziendale privacy sono coloro che coadiuveranno il Direttore Generale nella redazione del D.P.S. e nel governo della privacy aziendale.

I Responsabili del trattamento dei dati vengono designati con nota scritta dal Titolare, Istituto Nazionale per lo Studio e la Cura dei Tumori - Fondazione Giovanni Pascale, fra soggetti che per esperienza, capacità ed affidabilità, forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e che siano titolari:

- di un incarico di responsabilità di unità operativa complessa;

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

- di un incarico di responsabilità di unità operativa dipartimentale;
- di un incarico di referenza di uffici dotati di autonomia organizzativa e decisionale.

In particolare i Responsabili del trattamento sono tenuti:

- a comunicare tempestivamente al Referente Aziendale privacy l'inizio di ogni nuovo trattamento dei dati nonché la cessazione o la modifica dei trattamenti già in essere all'interno del proprio settore di competenza;
- a trasmettere entro il mese di febbraio di ogni anno la relazione sulle misure di sicurezza di cui al successivo art. 19, comma 2, lett. c.

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al proprio settore di competenza.

Responsabili esterni sono gli Enti, organismi, associazioni di volontariato, persone fisiche, strutture private accreditate, società di persone o di capitali, studi legali che in base a contratto od a convenzioni compiono) attività che comportano il trattamento di dati personali.

Incaricati del trattamento sono coloro i quali effettuano materialmente operazioni di trattamento di dati personali.

I Responsabili dei trattamenti in carica hanno individuato gli Incaricati al trattamento, tramite una Lettera d'incarico firmata dall'incaricato stesso.
Tutte le lettere d'incarico degli "incaricati" individuati dai Responsabili del trattamento dati delle UU.OO, Servizi, Settori amministrativi, sono custodite presso l'Ufficio Privacy incardinato presso la U.O.C. Affari Legali.
Gli incaricati sono stati informati a cura dei Responsabili del trattamento dati dei loro compiti e responsabilità ed effettueranno i corsi di formazione che saranno organizzati.

Elenco dei Responsabili Trattamento dati.

VEDI ALLEGATI B e C

8. INTERVENTI FORMATIVI.

8.1 Attività già effettuate.

- corso di formazione per gli operatori esterni addetti al servizio facchinaggio ed al servizio di prenotazione delle visite mediche;
- attività di docenza in occasione del convegno "Ricerca biomedica tra privacy e qualità" del 29/11/2011;
- attività di docenza in occasione del convegno "Il nuovo Sistema di Educazione Continua in Medicina: Criteri, Regole, e Procedure" del 20/12/2011;
- interventi di formazione per consulenze presso singole strutture aziendali.

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

- Nel corso del 2011, con deliberazione n. 628 del 30/06/2011 è stato adottato il Regolamento aziendale privacy unitamente ad un breve manuale che raccoglie una serie di indicazioni fornite dal Garante privacy nel corso degli anni.

8.2 Attività future.

Sono previste iniziative di formazione sui temi della 196/2003, diversificate per categoria d'utenza, in modo da affrontare, per ogni situazione specifica, le particolari problematiche. Il piano di formazione impostato è stato progettato con l'obiettivo di informare gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.
I contenuti previsti sono:
• informazioni sul D. Lgs. 196/2003, e sui principi legislativi comunitari;
• funzionamento della normativa nell'ambito dei diritti del cittadino e comportamenti aziendali;
• rischi possibili e probabili cui sono sottoposti i dati (con richiami a casi di crimini informatici, frodi, abusi, danni);
• misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi;
• comportamenti e modalità di lavoro per prevenire i rischi.
Tali interventi formativi sono programmati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze
• in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
• in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

8.3 Informativa capillare.

E' stato adottato un modello di informativa apposta in tutti i locali frequentati dall'utenza.

8.4 Pubblicazione su INTERNET.

A supporto dei Responsabili e degli Incaricati, al fine di risolvere eventuali problematiche connesse al D. Lgs. n°196/03 (Codice in materia di protezione sui dati personali), i documenti ufficiali relativi all'adeguamento al D.lgs. 196/03 sono pubblicati sul sito aziendale.

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

9. EVENTI E IMPATTI SULLA SICUREZZA.

Sono stati analizzati i principali eventi, intesi come minacce e vulnerabilità, e le relative conseguenze individuate per la sicurezza dei dati, in relazione a ciascun evento.

		Evento	Descrizione evento	Impatto sulla sicurezza
Eventi relativi al contesto fisico - ambientale	Eventi relativi alle sedi fisiche	Ingressi non autorizzati a locali/aree ad accesso ristretto	Possono verificarsi accessi non autorizzati da parte di persone che si trovano sia all'esterno che all'interno dell'organizzazione.	Accesso a documenti cartacei e strumenti.
		Sottrazione di strumenti contenenti dati	Strumenti contenenti dati (PC, portatili, supporti di memorizzazione,…) possono essere sottratti illecitamente da terzi.	Sottrazione di strumenti contenenti dati e quindi perdita di dati, in modo illecito.
		Sottrazione di credenziali di autenticazione	Grazie alla non curanza nella Conservazione delle credenziali di autenticazione (password scritte su post-it, su agende, su foglietti,…), queste possono essere sottratte al legittimo possessore e utilizzate in modo improprio.	Accesso alle banche dati (e quindi anche a dati particolarmente critici e/o sensibili) protette con tali credenziali
		Sottrazione di Documenti cartacei	Persone non autorizzate possono accedere a documenti cartacei incustoditi presenti su scrivanie, scaffali a vista, armadi non chiusi, archivi.	Sottrazione e accesso non autorizzato a dati o informazioni importanti o riservate.
		Calamità naturali	Terremoti, tempeste, inondazioni, fulmini e incendi possono causare danni gravi ai computer	Perdita di dati, tempi di inattività o perdite di produttività.
		Errori umani	A causa della mancanza di consapevolezza, incuria, distrazione gli utenti possono compiere operazioni errate.	Perdita, danneggiamento o alterazione di dati importanti.
	Eventi relativi ai locali CED	Ingressi non autorizzati	Possono verificarsi accessi non autorizzati da parte di persone che si trovano sia all'esterno che all'interno dell'organizzazione.	Sottrazione di strumenti contenenti dati. e quindi perdita di dati, in modo illecito.
		Sottrazione di strumenti contenenti dati	Strumenti contenenti dati (PC, portatili, supporti di memorizzazione,…) NON possono essere sottratti illecitamente da terzi.	Sottrazione di strumenti contenenti dati, e quindi perdita di dati, in modo illecito.
		Calamità naturali	Terremoti, tempeste,	Perdita di dati, tempi di

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

			inondazioni, fulmini e incendi possono causare danni gravi ai computer e ai dati contenuti	inattività o perdite di produttività.
		Rischi connessi a sistemi di climatizzazione	Possono verificarsi malfunzionamenti sui sistemi ausiliari necessari al corretto funzionamento degli apparati HW/SW con i quali viene trattata la banca dati interessata	Perdita parziale o totale dei dati.
		Errori umani nella gestione della sicurezza	A causa di disattenzione possono verificarsi errori nella gestione della sicurezza (lasciare i locali CED aperti e quindi accessibili a chiunque, mal gestione di strumenti,…).	Perdita, danneggiamento o alterazione di dati importanti.
		Manomissione/sabotaggio degli strumenti	Possono verificarsi manomissioni alle risorse hardware	Perdita di dati, tempi di inattività o perdite di produttività.
		Perdita di dati dovuta ad errori o a guasti	Errori di configurazione dell'hardware o guasti possono provocare malfunzionamenti alle risorse hardware.	Perdita di dati, tempi di inattività o perdite di produttività.
		Errori software / errori di Configurazione che minacciano l'integrità dei dati	Possono essere presenti nelle applicazioni errori involontari commessi in fase di progettazione e/o implementazione.	Accesso non autorizzato a dati o informazioni importanti o riservate, perdita di dati, manipolazione di dati, distruzione di dati.
		Presenza di codice non conforme alle specifiche del programma	Possono essere presenti applicazioni software che non offrono sufficienti garanzie di sicurezza.	Accesso non autorizzato a dati o informazioni importanti o riservate, perdita di dati, manipolazione di dati, distruzione di dati.
	Eventi relativi alle comunicazioni	Accesso non autorizzato alla rete	Soggetti non autorizzati possono accedere alla rete aziendale, agli applicativi e agli strumenti di interoperabilità.	Accesso non autorizzato a dati o informazioni importanti o riservate, perdita di dati, manipolazione di dati, distruzione di dati. Utilizzazione di servizi o risorse di rete.

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

		Intercettazione di informazioni transitanti sulla rete	Soggetti malintenzionati possono accedere a informazioni transitanti sulla rete.	Accesso non autorizzato a dati o informazioni importanti o riservate.
Eventi relativi al comportamento degli operatori.		Accesso non autorizzato ai Documenti cartacei	Persone non autorizzate possono accedere a documenti cartacei incustoditi presenti su scrivanie, scaffali a vista, armadi non chiusi, archivi.	Accesso non autorizzato a dati o informazioni importanti o riservate.
		Cancellazione non autorizzata di dati/manomissione di dati	A causa della mancanza di consapevolezza, incuria, distrazione gli utenti possono compiere operazioni errate.	Perdita, danneggiamento o alterazione di dati importanti.
		Sottrazione di credenziali	Password deboli possono essere indovinate da soggetti malintenzionati e utilizzate in modo improprio.	Accesso alle banche dati (e quindi anche a dati particolarmente critici e/o sensibili) protette con tali credenziali.
		Carenza di consapevolezza, disattenzione o incuria	A causa di incuria, disattenzione o scarsa conoscenza degli strumenti gli operatori possono digitare dati errati o compiere operazioni errate.	Perdita, danneggiamento o alterazione di dati importanti.
		Comportamenti sleali o fraudolenti	Gli utenti del trattamento possono compiere operazioni illecite, con comportamento consapevole, sulla banca dati interessata.	Perdita, danneggiamento o alterazione di dati importanti. Sottrazione di dati o informazioni importanti o riservate.

Istituto nazionale per lo studio e la cura dei tumori – Fondazione "G. Pascale" ---- Servizio Affari Legali
Via Mariano Semmola – 80131 – NAPOLI Tel. 081/59.03.421-222 – Fax 081/59.03.834
Direttore: avv. Carmine Mariano e-mail: c.mariano@istitutotumori.na.it
Referente aziendale privacy dr. Francesco Paolo Festa
Tel. 081.5903345 fax. 081/5903719 e-mail: f.festa@istitutotumori.na.it

10. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

Il D. lgs. 196/2003 ha per finalità quella di garantire che "il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".
Sulla base di quanto prescritto dal Codice, vengono individuati tre requisiti di sicurezza, che costituiscono il riferimento per valutare il proprio grado di corrispondenza rispetto a quanto indicato dal D. lgs. 196/2003.

I tre requisiti sono:
riservatezza: requisito specificatamente indicato nelle finalità del D. lgs. 196/2003, si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati di natura personale e sensibile da modalità di trattamento non autorizzato che contemplano il rischio di accesso ai dati, e rientranti nelle seguenti categorie di attività specificatamente indicate dalla legge:

raccolta,
registrazione,
organizzazione,
conservazione,
comunicazione,
diffusione
selezione,
estrazione,
raffronto,
interconnessione,
utilizzo

integrità: tale requisito si riferisce alla possibilità di intraprendere azioni in grado di proteggere i dati di natura personale e sensibile da modalità di trattamento non autorizzate che contemplano il rischio di modifica delle informazioni, e rientranti nelle seguenti categorie di attività specificatamente indicate dalla Legge:

- elaborazione,
- modificazione,
- cancellazione,
- blocco,
- distruzione.

disponibilità: tale requisito si riferisce alla necessità di intraprendere azioni in grado di proteggere dati personali, sensibili e giudiziari da possibili eventi che possono ridurre la capacità dell'Azienda di assolvere alle finalità di trattamento per cui tali dati sono stati raccolti.
Tali requisiti forniscono quindi un punto di partenza per l'identificazione dei possibili attacchi, individuabili in base all'analisi dello scenario effettuata, e servono alla definizione dei criteri di protezione più adeguati a garantire tale necessità di protezione.
Per Analisi dei Rischi si intende l'attività di raccolta ed analisi delle minacce e delle vulnerabilità a cui sono soggette le risorse nel rispetto del CODICE.
In questa sezione viene data una valutazione qualitativa dei rischi. Al risultato si è arrivati grazie alla combinazione di questionari e interviste aperte che hanno coinvolto gruppi diversificati di persone che operano all'interno dell'Azienda.
Il **rischio da abbattere** è la probabilità che si verifichi un impatto sulle attività aziendali.

Probabilità evento	Descrizione
0	Poco probabile
1	Probabile
2	Verosimile

Rischio da abbattere

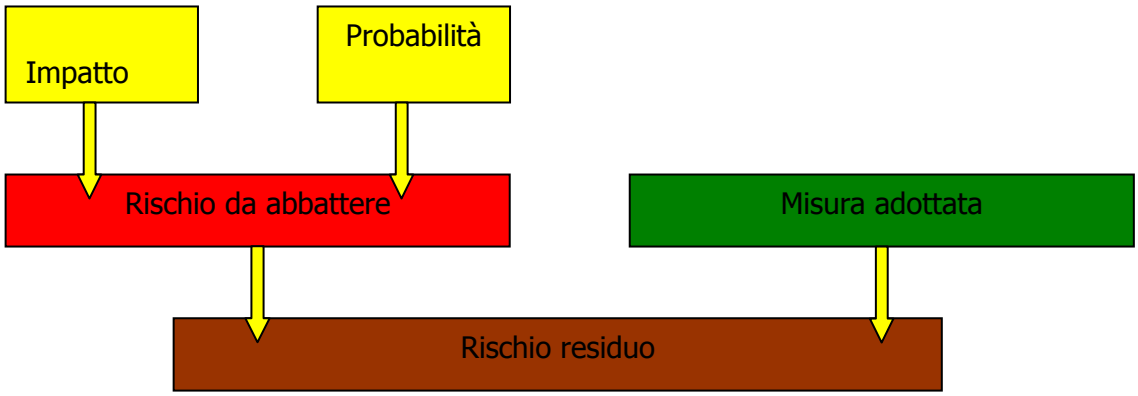
Livello impatto	Descrizione
0	Impatto basso
1	Impatto medio
2	Impatto alto

Impatto

2	0	2	4
1	0	1	2
0	0	0	0
	0	1	2

Probabilità

Il **rischio residuo** ritenuto accettabile, valutato per ogni singolo evento, è calcolato considerando il rischio da abbattere insieme con le eventuali misure adottate.
Il **rischio residuo** è un rischio che permane anche quando sono state applicate le misure di sicurezza.



Il **rischio residuo** è:

	Rischio residuo basso: livello di rischio accettabile

	Rischio residuo medio: il rischio non è totalmente o parzialmente contrastato. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio residuo.
	Rischio residuo alto: è inaccettabile. Pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, etc..) per abbattere il rischio residuo e contenerlo in livelli accettabili.

L'esistenza di un **rischio residuo** (indipendentemente che sia basso, medio o alto) significa prendere atto che la sicurezza assoluta non è un obiettivo conseguibile.
Pertanto è necessario prevedere, accanto alle misure adottate, anche le modalità di gestione dell'evento e quella delle situazioni post evento, nelle quali deve trovare spazio la convivenza con una quota non eliminabile di **rischio residuo**.
Nella tabella seguente viene calcolato il rischio residuo dell'Azienda.

		Evento	Impatto (0-2)	Prob. (0-2)	Rischio da abbattere IxP (0-4)	Misure adottate	Rischio residuo
ANALISI DEI RISCHI RELATIVI AL CONTESTO FISICO-AMBIENTALE	Analisi dei rischi sulle sedi fisiche	Ingressi non autorizzati a locali/aree ad accesso ristretto	2	1	2	M01 M02 M03	
		Sottrazione di strumenti contenenti dati	2	0	0	M01 M02 M03	
		Sottrazione di credenziali di Autenticazione	2	0	0	M02	
		Sottrazione di documenti cartacei	2	1	2	M01 M02 M03 M15 M21	
		Calamità naturali	2	0	0	M04	
		Errori umani	1	1	1	M13	
	Analisi dei rischi nei	Ingressi non autorizzati	1	1	1	C01 C02	
		Sottrazione di strumenti	2	0	0	C01 C02	

		contenenti dati					
		Calamità naturali	2	0	0	C03 C05	
		Rischi connessi a sistemi di Climatizzazione	1	1	1	C04	
		Errori umani nella gestione della sicurezza	1	1	1	C06	
ANALISI DEI RISCHI RELATIVI AGLI STRUMENTI	Analisi dei rischi sulle risorse hardware	Uso non autorizzato dell'hardware o di strumenti	1	1	1	M07	
		Sottrazione di credenziali di autenticazione	2	1	2	M07 M08	
		Perdita di dati dovuta ad errori o a guasti	2	1	2	M01 M02 M03 M11	
		Perdita di dati dovuta ad errori o a guasti	2	1	4	M13 M19 M20 M21	
		Rischi connessi all'elettricità	2	1	4	M06	
	Analisi dei rischi sulle risorse software	Accesso non autorizzato alle basi dati connesse	2	1	4	M07 M08 M10	
		Errori software / errori di configurazione che minacciano l'integrità dei dati	2	1	4	M12	
		Presenza di codice non conforme alle specifiche del programma	2	1	4	M14	
		Azione di virus informatici	2	1	4	M14	
	Analisi dei	Accesso non autorizzato alla rete	2	1	4	M07 M08 M09 M21	

		Intercettazione di informazioni transitanti sulla rete	2	1	4	M10	
ANALISI DEI RISCHI RELATIVI AI COMPORTAMENTI DEGLI		Accesso non autorizzato ai documenti cartacei	2	1	4	M01 M15 M21	
		Accesso non autorizzato ai dati	2	1	4	M01 M05 M17 M18 M19 M20	
		Cancellazione non autorizzata di dati/manomissione di dati	2	1	2	M07 M08	
		Sottrazione di credenziali	2	1	2	M07 M08	
		Carenza di consapevolezza, disattenzione o incuria	2	1	2	M16	
		Comportamenti sleali o fraudolenti	2	0	0	M16	

11. MISURE DI SICUREZZA IN ESSERE.

Al fine di assicurare:

- l'integrità e la disponibilità dei dati;
- la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento ed impedirne la comunicazione e/o diffusione non autorizzata;

l'Azienda ha elaborato nel corso degli ultimi anni una Politica di Sicurezza basata sull'adozione di misure di tipo fisico, logico ed organizzativo. Tali misure hanno il compito di garantire sia i minimi requisiti di sicurezza contemplati dal Codice, sia un livello idoneo di sicurezza relativamente alle tipologie dei dati trattati, alle modalità di trattamento ed agli strumenti utilizzati.

LOCALI CED

C01	Misure di sicurezza di tipo fisico
Misura adottata	La sala macchine presente all'interno dell'area CED, non è accessibile da personale esterno in quanto è stata dotata di porta dotata di serratura. La porta è tagliafuoco. Gli armadi di rete sono protetti da eventuali accessi non autorizzati in quanto dotati di serratura.
Evento che si intende contrastare	Ingressi non autorizzati a locali/aree ad accesso ristretto Sottrazione di strumenti contenenti dati
Trattamenti interessati	Trattamenti informatici

C02	Accesso ai locali
Misura adottata	L'accesso ai locali nei quali sono ospitati i sistemi di elaborazione o i sistemi di comunicazione è interdetto a chiunque, fatta eccezione per il personale autorizzato. Se eventualmente si rendesse necessario l'accesso a detti locali da parte di personale non autorizzato - per es. da parte di tecnici della manutenzione di ditte fornitrici, ecc., i visitatori vengono opportunamente identificati e accompagnati durante tutta la loro permanenza in detti locali da personale autorizzato. Deroghe a tale regola potranno essere concesse solo dietro precisa motivazione e andranno comunque segnalate al Responsabile della sicurezza dei dati e dei sistemi.
Evento che si intende contrastare	Ingressi non autorizzati a locali/aree ad accesso ristretto Sottrazione di strumenti contenenti dati
Trattamenti interessati	Trattamenti informatici

C03	Misure di protezione da eventi di origine naturale o dolosa

Misura adottata	I locali CED sono dotati di un idoneo numero di estintori. Il pavimento della sala server è flottante e antistatico.
Evento che si intende contrastare	Evento di origine naturale o dolosa
Trattamenti interessati	Tutti i trattamenti

C04	Climatizzazione dei locali
Misura adottata	La sala macchine è dotata di impianto di climatizzazione opportunamente dimensionato.
Evento che si intende contrastare	Rischi connessi a sistemi di climatizzazione
Trattamenti interessati	Trattamenti di tipo informatico

C05	Continuità dell'alimentazione elettrica
Misura adottata	E' garantita la presenza di gruppo di continuità in grado di fungere da backup per brevi interruzioni di energia elettrica.
Evento che si intende contrastare	Rischi connessi all'elettricità
Trattamenti interessati	Trattamenti di tipo informatico

C06	Continuità del servizio
Misura adottata	I server hanno dischi mirrorati in alta affidabilità.
Evento che si intende contrastare	Perdita di dati
Trattamenti interessati	Trattamenti di tipo informatico

Altri locali

M01	Misure di protezione delle aree e dei locali
Misura adottata	Alcune sedi sono protette da un sistema di allarme antintrusione. Durante le ore notturne il controllo di tutte le sedi è affidato ad un servizio di vigilanza tramite personale addetto. I locali dispongono di un'area destinata alla ricezione del pubblico. I locali sono costantemente presidiati dal personale durante il giorno.

	Allo scadere dell'orario di sportello, le porte di accesso vengono chiuse e nessun utente dei servizi è ammesso, se non personalmente accompagnato da personale autorizzato. Il personale dipendente ogni giorno timbra l'entrata/uscita per l'accesso agli uffici; per gli utenti ed i visitatori non esiste una registrazione ad eccezione degli uffici che erogano servizi al pubblico, le cui modalità sono diversificate in funzione dei servizi erogati agli utenti che usufruiscono delle prestazioni.
Evento che si intende contrastare	Ingressi non autorizzati a locali/aree ad accesso ristretto Sottrazione di strumenti contenenti dati Sottrazione di documenti cartacei Manomissione/sabotaggio degli strumenti Accesso non autorizzato ai documenti cartacei
Trattamenti interessati	Tutti i trattamenti
Struttura o persone addette all'adozione	Tutte le sedi

M02	Accesso ai locali
Misura adottata	I flussi relativi a personale NON dipendente sono identificabili in due tipologie: gli assistiti ed eventuali parenti o affini ed i terzi prestatori d'opera (dipendenti di imprese esterne,consulenti, ecc). In entrambi i casi il personale consente loro l'accesso ai locali filtrandoli al momento del loro ingresso. Gli addetti sono tenuti ad effettuare vigilanza contro il rischio di accesso di persone non autorizzate.
Evento che si intende contrastare	Sottrazione di strumenti contenenti dati Sottrazione di documenti cartacei Manomissione/sabotaggio degli strumenti Ingressi non autorizzati a locali/aree ad accesso ristretto
Trattamenti interessati	Tutti i trattamenti
Struttura o persone addette all'adozione	Tutte le sedi

M03	Registrazione degli accessi
Misura	Il personale dipendente ogni giorno timbra l'entrata/uscita per l'accesso agli

adottata	uffici; per gli utenti ed i visitatori non esiste una registrazione ad eccezione degli uffici che erogano servizi al pubblico le cui modalità sono diversificate in funzione dei servizi erogati agli utenti che usufruiscono delle prestazioni.
Evento che si intende contrastare	Sottrazione di strumenti contenenti dati Sottrazione di documenti cartacei Manomissione/sabotaggio degli strumenti Ingressi non autorizzati a locali/aree ad accesso ristretto
Trattamenti interessati	Tutti i trattamenti
Struttura o persone addette all'adozione	Tutte le sedi

M04	Misure di protezione da eventi di origine naturale o dolosa
Evento che si intende contrastare	Calamità naturali
Trattamenti interessati	Tutti i trattamenti
Struttura o persone addette all'adozione	Tutte le sedi

M05	Misure di protezione per il rispetto dei diritti dell'interessato
Misura adottata	L'Azienda, nell'organizzazione delle prestazioni e dei servizi erogati ha attivato un processo di adeguamento attraverso l'adozione di idonee misure volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale. Tale processo di adeguamento comprende: Soluzioni rivolte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno delle strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa; Adozione di appropriate distanze di cortesia. Soluzioni per la prevenzione, durante i colloqui, dell'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute; Adozione di cautele volte ad evitare che le prestazioni sanitarie, compresa

	l'eventuale anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti; Rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati; Previsione, in conformità all'ordinamento interno delle strutture ospedaliere, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettandone eventuali loro contrarie manifestazioni legittime di volontà; Adozione di procedure, anche di formazione del personale, dirette a prevenire ,nei confronti di personale estraneo, un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute; Sottoposizione da parte degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.
Evento che si intende contrastare	Accesso non autorizzato ai dati
Trattamenti interessati	Tutti i trattamenti
Struttura o persone addette all'adozione	Tutte le sedi

M06	Continuità dell'alimentazione elettrica
Misura adottata	Server esterni ai locali CED e gestiti dal personale dei Sistemi informativi. I server in gestione al personale dei Sistemi informativi, sono tutti collegati ad un gruppo di continuità. Server esterni ai locali CED non gestiti dal personale dei Sistemi informativi I server esterni ai locali CED non gestiti dal personale dei Sistemi informativi, sono quasi tutti collegati ad un gruppo di continuità.
Evento che si intende contrastare	Rischi connessi all'elettricità
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Uffici di tutte le sedi

M07	Credenziali
Misura adottata	Al momento non esiste un sistema centralizzato di gestione delle credenziali di accesso. Detta gestione è affidata ad ogni singolo utente/reparto. I sistemi operativi consentono una corretta gestione delle passwords di autenticazione. La maggior parte delle applicazioni sia centralizzate che locali gestiscono la profilazione degli utenti a livello individuale e/o di gruppo, consentendo il rispetto degli ambiti di trattamento autorizzati
Evento che si intende contrastare	Uso non autorizzato dell'hardware Accesso non autorizzato alle basi dati connesse Cancellazione non autorizzata di dati/manomissione di dati Sottrazione di credenziali Accesso non autorizzato alla rete
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M08	Gestione e controllo dei posti di lavoro
Misura adottata	Attualmente l'Azienda manca di strumenti specifici di gestione dei posti di lavoro (alcuni dei quali tra l'altro facenti funzioni di server e contenenti dati rilevanti) sulla rete geografica. In caso di anomalia o malfunzionamento può essere necessario inviare sul posto un addetto del Sistema Informatico.
Evento che si intende contrastare	Accesso non autorizzato alle basi dati connesse Cancellazione non autorizzata di dati/manomissione di dati Sottrazione di credenziali Accesso non autorizzato alla rete
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M09	Accesso ad Internet
Misura adottata	L'accesso ad Internet e l'utilizzo della mail da parte di un nuovo Incaricato sono subordinati ad una richiesta scritta, autorizzata dal Responsabile del trattamento (o dal Dirigente funzionale dell'incaricato). La navigazione degli utenti è gestita da un Proxy SQUID.
Evento che si intende contrastare	Accesso non autorizzato alle basi dati connesse
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M10	Protezione da accessi non autorizzati provenienti da Internet
Misura adottata	L'AZIENDA utilizza un firewall dedicato, installato e gestito direttamente dal personale dei Sistemi informativi i, che adotta procedure di controllo costante delle risorse hardware e software. I manutentori dei software applicativi sono autorizzati ad accedere solo alle procedure e ai dati di loro competenza, ma non vi sono particolari protezioni contro l'accesso doloso a dati non autorizzati. I manutentori esterni accedono alla rete tramite VPN. Il collegamento avviene in maniera criptata. Ciascuna persona esterna accede con una propria password, e gli accessi vengono tracciati in un file di log: tali accessi vengono autorizzati dal CED fino a revoca.
Evento che si intende contrastare	Accesso non autorizzato alle basi dati connesse Intercettazione di informazioni transitanti sulla rete
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M11	Accesso agli strumenti
Misura adottata	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia. L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (per es. perché

	impegnato in compiti che richiedono totalmente la sua attenzione).
Evento che si intende contrastare	Manomissione/sabotaggio degli strumenti
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M12	Errori noti del software
Misura adottata	I software sono utilizzati da parecchi anni e non hanno mai causato la perdita o il danneggiamento dei dati trattati.
Evento che si intende contrastare	Errori software che minacciano l'integrità dei dati
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M13	Aggiornamento dei programmi software
Misura adottata	Elaboratori gestiti dal personale del Servizio informatica . Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, sono effettuati periodicamente, almeno una volta ogni dodici mesi e comunque quando disponibile o necessario, ma sempre dopo aver concordato l'intervento con il personale interno che vi sovrintende. Elaboratori non gestiti dal personale del Servizio informatico. Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, gestiti localmente dai Responsabili sono effettuati periodicamente, almeno una volta ogni dodici mesi.
Evento che si intende contrastare	Perdita di dati dovuta ad errori o a guasti Errori umani
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M14	Protezione posti di lavoro

Misura adottata	La protezione di tutti i posti di lavoro collegati alla rete, dei server e delle postazioni mobili viene assicurata attraverso un certo numero di antivirus che garantiscono l'aggiornamento automatico del Data Base dei virus attraverso un collegamento al sito che viene attivato con frequenza giornaliera. L'antivirus è settato per la protezione in tempo reale sui files e messaggi in ingresso. La scansione sui posti di lavoro viene effettuata con frequenza almeno giornaliera. E' presente inoltre un sistema antivirus sul server di posta.
Evento che si intende contrastare	Azione di virus informatici Presenza di codice non conforme alle specifiche del programma
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M15	Protezione dei dati cartacei
Misura adottata	Quando gli atti e i documenti contenenti dati personali sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione. Gli atti e i documenti vengono restituiti al termine delle operazioni affidate, ovvero ricollocati nel posto in cui sono stati prelevati (ad es. archivio o schedario delle pratiche in corso). Eventuali fotocopie o copie di documenti sono custodite con le stesse modalità dei documenti originali. La distruzione definitiva dei documenti cartacei avviene in modo controllato ed in modalità tale da assicurare il non riutilizzo dei dati.
Evento che si intende contrastare	Accesso non autorizzato ai documenti cartacei
Trattamenti interessati	Trattamenti di tipo cartaceo
Struttura o persone addette all'adozione	Tutte le sedi

M16	Formazione e informazione del personale

Misura adottata	Il Regolamento Aziendale e il D.P.S. sono disponibili sul sito web aziendale . I Responsabili del trattamento hanno il compito di informare tutti gli operatori della propria U.O. – Servizio Sono previsti incontri formativi di sensibilizzazione, informazione e aggiornamento agli incaricati e Responsabili sulla corretta modalità operativa per il trattamento dei dati e sui nuovi strumenti e /o misure di sicurezza implementati in azienda.
Evento che si intende contrastare	Carenza di consapevolezza, disattenzione o incuria Comportamenti sleali o fraudolenti
Trattamenti interessati	Tutti i trattamenti
Struttura o persone addette all'adozione	Tutte le sedi

M17	Gestione delle prescrizioni mediche
Misura adottata	Alle ricette mediche si applicano le norme del Titolo V , Capo IV ,del Codice.
Evento che si intende contrastare	Accesso non autorizzato ai dati
Trattamenti interessati	Trattamenti di tipo cartaceo
Struttura o persone addette all'adozione	Tutte le sedi

M18	Gestione della cartella clinica
Misura adottata	Nella cartella clinica, in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati.
Evento che si intende contrastare	Accesso non autorizzato ai dati
Trattamenti interessati	Trattamenti di tipo cartaceo
Struttura o persone addette all'adozione	Tutte le sedi

M19	Salvataggio dati
Misura adottata	Dati residenti sui server presso i locali CED. Gli archivi informatici contenenti dati personali vengono salvati dall'incaricato del salvataggio su un set minimo di supporti per i salvataggi a rotazione, secondo una metodica che consente di disporre in ogni momento delle copie di salvataggio. Dati residenti sui server esterni ai locali CED ma gestiti dal personale del Servizio informatica Salvataggio giornaliero a cura del personale del Servizio Informatica e telecomunicazioni. Dati sui server locali non gestiti dal personale del Servizio informatica : Salvataggio giornaliero a carico dei singoli servizi
Evento che si intende contrastare	Perdita di dati dovuta ad errori o a guasti Errori umani
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M20	Protezione risorse software
Misura adottata	Le misure adottate per proteggere l'efficienza e l'efficacia delle risorse software, consistono in: - utilizzo di software specialistico per preservare l'integrità dei dati quali, l'antivirus e il software per il recupero dei dati accidentalmente o volontariamente cancellati. - attività periodica di backup su supporti informatici.
Evento che si intende contrastare	Perdita di dati Accesso non autorizzato alla rete
Trattamenti interessati	Trattamenti di tipo informatico
Struttura o persone addette all'adozione	Tutte le sedi

M21	Protezione archivi cartacei
Misura adottata	Archivio corrente Le aree contenenti dati cartacei sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone non autorizzate e, di conseguenza, impedirne l'accesso stesso. Archivio di deposito Gli archivi di deposito normalmente vengono tenuti chiusi a chiave; vi può accedere solo il personale autorizzato. Archivio storico L'accesso agli archivi storici segue le norme previste per le aree di sicurezza ed è consentito esclusivamente a personale autorizzato.
Evento che si intende contrastare	Accesso non autorizzato ai documenti cartacei
Trattamenti interessati	Trattamenti di tipo cartaceo
Struttura o persone addette all'adozione	Tutte le sedi

12. CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI.

12. 1 PROCEDURE PER IL SALVATAGGIO REGOLARE DEI DATI.

Il salvataggio dei dati è una procedura che ricopre una funzione cruciale. Attraverso questa procedura, è possibile, in caso di guasto hardware dei dischi, "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo salvataggio

Gestione centralizzata	Salvataggio dati residenti sui server presso i locali CED	Gli archivi informatici contenenti dati personali vengono salvati dal personale del Servizio informatica e su un set minimo di supporti per i salvataggi a rotazione, secondo una metodica che consente di disporre in ogni momento delle copie di salvataggio.
	Salvataggio dati residenti sui server esterni ai locali CED ma gestiti dal personale del Servizio informatica	Salvataggio giornaliero su cassetta a cura del personale del Servizio informatica e telecomunicazioni
Gestione locale	Salvataggio dati sui server locali non gestiti dal personale del Servizio informatica	Salvataggio giornaliero a carico del Responsabile della singola unità operativa o personale delegato

12.2 PROCEDURE PER L'ARCHIVIAZIONE DEI SUPPORTI DI MEMORIZZAZIONE.
I supporti di memorizzazione vengono etichettati con informazione per l'identificazione e conservati.

12.3 PROCEDURE PER LA VERIFICA DELLA LEGGIBILITÀ DEI SUPPORTI DI MEMORIZZAZIONE.

La verifica dell'integrità dell'informazione memorizzata viene eseguita manualmente dall'incaricato al salvataggio.

12.4 CRITERI PER L'ELIMINAZIONE DEI SUPPORTI DI MEMORIZZAZIONE OBSOLETI.
In generale i supporti di memorizzazione – anche non removibili - che contengono dati personali o sensibili, nel caso non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dimessi – per es. per obsolescenza o per guasto -, dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

12.5 PROVE DI RIPRISTINO.
Periodicamente dovranno essere eseguite prove di ripristino dei dati dall'Incaricato delle copie di sicurezza.

12.6 PIANO DI CONTINUITÀ OPERATIVA.
L'obiettivo del piano di continuità operativa è quello di garantire la continuità del servizio informatico e la disponibilità delle informazioni, evitando o limitando i danni al patrimonio informativo a fronte di una emergenza.
Il piano di continuità operativa non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime.
Allo scopo di gestire gli eventi critici e i disastri quali cessazione temporanea della corrente elettrica, presenza di Virus informatici provenienti da fonti esterne (Internet, floppy ecc…) per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, l'AZIENDA ha adottato le seguenti misure:

- server con dischi ridondati o in cluster;
- salvataggio dei dati;
- etichettatura dei supporti di memorizzazione con informazione per l'identificazione;
- verifica dell'integrità dell'informazione memorizzata;
- Il piano prevede nell'eventualità che un incidente comprometta la sicurezza dei sistemi, figure professionali altamente qualificate quali i manutentori dei sistemi stessi, che sono in grado di intervenire per limitare e/o eliminare eventuali problemi causati dall'evento

13. CRITERI PER LA CIFRATURA O PER LA SEPARAZIONE DI DATI.
La Azienda essendo un'azienda pubblica che eroga servizi sanitari, è soggetta all'osservanza dei criteri di cifratura separazione dei dati come richiesto dal CODICE.

L'Azienda sta valutando l'implementazione di un sistema, anche in considerazione di esperienze messe in atto o in corso di studio in altre Aziende Sanitarie, per applicare quanto previsto dal CODICE in merito alla cartella clinica e ai campioni biologici e istologici e alle radiografie.

14. MISURE DI SICUREZZA DA ADOTTARE.

Misure da adottare	**Rischi da contrastare**	**Trattamenti interessati**	**Struttura o persone addette all'adozione**	**Tempi previsti per la messa in opera**
Migliorare la gestione delle credenziali di autenticazione, estendendo i meccanismi di scadenza automatica delle stesse a tutti i PC. Proseguire l'istruzione degli incaricati sulle corrette modalità di gestione autonoma delle credenziali. Proseguire l'istruzione degli incaricati sulla corretta gestione degli strumenti elettronici.	Uso non autorizzato dell'hardware Accesso non autorizzato alle basi dati connesse Cancellazione non autorizzata di dati/manomissione di dati Sottrazione di credenziali Accesso non autorizzato alla rete	Trattamenti di tipo informatico	Tutte le sedi	In itinere
Scelta e adozione di strumenti di single sign on.	Uso non autorizzato dell'hardware Accesso non autorizzato alle basi dati connesse Cancellazione non autorizzata di dati/manomissione di dati Sottrazione di credenziali Accesso non autorizzato alla rete	Trattamenti di tipo informatico	Tutte le sedi	Da Pianificare

Migliorare la gestione dei profili di autorizzazione, con particolare riferimento alla gestione degli stessi da parte delle applicazioni informatiche più datate.	Uso non autorizzato dell'hardware Accesso non autorizzato alle basi dati connesse Cancellazione non autorizzata di dati/manomissione di dati. Sottrazione di credenziali Accesso non autorizzato alla rete	Trattamenti di tipo informatico	Tutte le sedi	In Itinere
Si intende avviare lo studio di fattibilità per migliorare il livello di protezione dei dati da perdita o danneggiamento, attraverso l'utilizzo di sistemi per duplicare, in sede diversa dal CED, la scrittura dei dati critici presenti sui DB centralizzati.	Calamità naturali Perdita o danneggiamento di dati, anche involontario	Trattamenti di tipo informatico	CED	Da Pianificare

15. PERIODICITA' DI REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il Documento Programmatico deve essere sottoposto a revisione e aggiornato entro il 31 marzo di ogni anno. Trascorso tale termine deve essere oggetto di revisione per adeguarlo ad eventuali variazioni del livello di rischio a cui sono soggetti i dati personali e ad eventuali modifiche della tecnologia informatica.
Nell'attesa dell'adeguamento conservano validità le regole in vigore.