SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Modena

Documento Programmatico sulla Sicurezza

Azienda Ospedaliero – Universitaria Di Modena

ai sensi del Codice in materia di protezione dei dati personali art. 34
e Allegato B, regola 19, del d.lg. 30 giugno 2003, n. 196
Predisposto il 24/05/2018

Riferimento documentale	
Titolo del documento	Documento Programmatico sulla sicurezza dell'Azienda Ospedaliero Universitaria di Modena
Numero di versione	1.3
Data Pubblicazione	24/05/2018
Stato del documento	Approvato
Redatto da	Ing. Roberto Savigni
Autorizzato da	Ing. Mario Lugli
Verificato da	

Indice generale

1. Principali riferimenti normativi

Nella stesura del documento sono stati considerati i principali riferimenti normativi vigenti in materia, relativamente a:

Protezione dei dati personali (D. Lgs. 196/2003 Codice Privacy), in particolare:

- **Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari**
  […] 6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
- **Art. 31. Obblighi di sicurezza**
  1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- **Art. 33. Misure minime**
  1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.
- ·**Art. 34. Trattamenti con strumenti elettronici**
  1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato A), le seguenti misure minime:
  a) autenticazione informatica;
  b) adozione di procedure di gestione delle credenziali di autenticazione;
  c) utilizzazione di un sistema di autorizzazione;
  d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
  e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
  f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
  g) [soppressa]
  h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari. [...]
- **Allegato B, paragrafo 19**1 (paragrafo ora abrogato dal D. L. 9 febbraio 2012, n. 5, convertito nella L. 4 aprile 2012, n. 35).
- **Regolamento Regionale sui dati sensibili e giudiziari,** adottato dalla Regione Emilia Romagna con Deliberazione n. 424 del 31/03/2014

Regolamento Europeo in materia di protezione dei dati (679/2016) - GDPR

Documenti informatici, misure di disaster recovery e business continuity, D. Lgs. 82/2005 s.m.i. (Codice dell'Amministrazione Digitale)
Crimine informatico
Tutela del diritto d'autore
Tenuta del protocollo informatizzato e gestione documentale
Uso dei supporti ottici

2. Introduzione

Vista la normativa in materia di trattamento di dati personali ed in particolare il Decreto legislativo 30 giugno 2003 n. 196 e il Disciplinare tecnico in materia di misure minime di sicurezza, al fine di ottemperare alla normativa ora richiamata l'Azienda Ospedaliero-Universitaria di Modena quale Titolare del trattamento dati redige il presente Documento Programmatico Sulla Sicurezza (DPSS) che definisce la Politica aziendale in materia di Privacy e le Misure di sicurezza approntate dall' Azienda medesima per garantire il livello minimo di sicurezza nel trattamento dei dati personali.

Il DPSS, da custodirsi presso la sede dell'Azienda, è a data certa e deve essere oggetto di rinnovo entro il 31 marzo di ogni anno.

Il presente documento deve essere conosciuto ed applicato dal Titolare, dai Responsabili e dagli Incaricati nominati, ciascuno secondo le proprie competenze.

L'Azienda Ospedaliero-Universitaria di Modena, struttura di integrazione tra Servizio Sanitario Nazionale e Università, ha così identificato la propria missione: L`Azienda Ospedaliero-Universitaria di Modena, nell'ambito del sistema regionale per la salute e per i servizi sociali, esercita le proprie funzioni assistenziali (di diagnosi, cura, riabilitazione e prevenzione), di ricerca biomedica e sanitaria e di formazione e didattica in integrazione con l`Università, in coordinamento e piena collaborazione con la Azienda USL di Modena e con le espressioni istituzionali e associative della comunità in cui opera.

Attraverso una risposta clinica e assistenziale appropriata e di qualità, costruita attorno ai bisogni dell'utente e allo sviluppo della sua funzione di ricerca e didattica, l`Azienda intende raggiungere i propri principali obiettivi ed in particolare:

a) sviluppare la propria capacità di diagnosi, cura, riabilitazione e prevenzione e, più in generale, di soddisfazione dei bisogni di salute delle persone che si rivolgono all'Azienda, al massimo livello qualitativo possibile, in modo appropriato, efficiente ed efficace;

b) sviluppare, nell'ambito dell'integrazione con l'Università, percorsi che favoriscano l'attuazione di processi di ricerca, formazione e di didattica di alta qualità;

c) consolidare la leadership dal punto di vista scientifico, diagnostico e di cura all'interno del contesto regionale e nazionale;

d) qualificarsi maggiormente come Ospedale di eccellenza nella Regione per completezza e per la complessità dei servizi erogati;

e) promuovere la cultura della sicurezza del paziente e degli operatori per portare l`Ospedale ai più elevati livelli possibili nel governo clinico e nell'organizzazione del lavoro.

La promozione della qualità, dell'appropriatezza, dell'efficienza, dell'efficacia, della valorizzazione delle risorse e della sicurezza costituisce il principio fondante a cui si ispira l`azione di governo aziendale, unitamente al perseguimento dei valori di universalità ed equità di accesso alle prestazioni, di rispetto dei principi di dignità della persona e di centralità del cittadino e del paziente.

L'Azienda persegue l'integrazione tra le diverse forme di assistenza sanitaria e sociale e la ricerca della cooperazione e del coinvolgimento di tutte le componenti rappresentative espresse dal contesto di riferimento.

L'Azienda vuole utilizzare tutti gli strumenti che permettano di promuovere e valorizzare la motivazione negli operatori e lo sviluppo delle relazioni interne, coinvolgendo le diverse espressioni professionali nei processi di sviluppo e miglioramento dell'organizzazione del lavoro e della qualità dei servizi.

La valorizzazione dei professionisti, lo sviluppo professionale e tecnologico e l'adeguamento delle competenze all`evoluzione scientifica costituiscono obiettivi prioritari per accrescere il ruolo di eccellenza nel panorama sanitario regionale e nazionale per le proprie funzioni di cura e nell'ambito della integrazione con la Università di formazione, didattica e ricerca.

In tale contesto l'Azienda garantisce il diritto alle attività libero professionali dei dirigenti a rapporto esclusivo, assicurando un corretto ed equilibrato rapporto tra attività istituzionale e libero professionale, nel rispetto della normativa e dei CC.CC.NN.LL vigenti.

I principali impegni che l'Azienda ha fatto propri ed intende sviluppare a beneficio dei cittadini sono:

- competenza, eccellenza e autorevolezza professionale;
- ascolto e coinvolgimento;
- motivazione e valorizzazione del capitale intellettuale;
- integrazione e sinergie multidisciplinari e interprofessionali;
- alta affidabilità, qualità, sicurezza e appropriatezza delle prestazioni;
- innovazione tecnologica e organizzativa;
- integrazione ospedale università;
- consolidamento dei rapporti con le strutture sanitarie della rete provinciale e regionale e forte integrazione con l'Azienda USL di Modena nella ricerca di sinergie per il raggiungimento di obiettivi comuni;
- coerenza della programmazione e della pianificazione con le indicazioni espresse dalla Conferenza Territoriale Sociale e Sanitaria;
- qualità del sistema di governo aziendale;
- equilibrio economico finanziario.

L'Azienda Ospedaliero-Universitaria di Modena è struttura di integrazione con l'Università degli Studi di Modena e Reggio. Pur non configurandosi alcuna fattispecie di contitolarità nel trattamento dei dati, si ritiene opportuno evidenziare brevemente le caratteristiche di tale integrazione.

In attuazione dell'art. 9 della Legge Regionale n. 29/2004, la Regione Emilia - Romagna e le Università degli Studi di Bologna, Ferrara, Modena - Reggio Emilia e Parma hanno sottoscritto il nuovo "Protocollo d'intesa", approvato con deliberazione della Giunta Regionale II. 297/2005, individuando nella integrazione la modalità idonea per realizzare il concorso delle rispettive autonomie.

In sede locale, l'Azienda e la Università definiscono il conseguente Accordo Attuativo che sviluppa i principi e le regole generali contenute nel citato Protocollo d'intesa.

L'Accordo Attuativo realizza l`integrazione informandosi al principio della leale collaborazione tra l'Azienda e l'Università, inteso come:

a) pieno coinvolgimento di tutte le componenti interessate nella realizzazione degli obiettivi della programmazione sanitaria nazionale, regionale e locale;

b) sviluppo di metodi e strumenti di collaborazione volti a perseguire, in modo integrato, obiettivi di:
   - qualità, efficienza, efficacia, appropriatezza delle prestazioni
   - qualità e congruità della didattica
   - potenziamento della ricerca biomedica e sanitaria;

c) impegno alla programmazione coordinata degli obiettivi e delle risorse in funzione delle attività assistenziali dell'Azienda e delle attività didattiche e di ricerca della Facoltà di Medicina e Chirurgia.

In particolare l'Accordo Attuativo locale individua:

- le strutture complesse a direzione universitaria e a direzione ospedaliera;
- l'afferenza alle strutture aziendali dei professori e dei ricercatori universitari nonché delle figure equiparate;
- la istituzione dei Dipartimenti ad Attività Integrata, con la identificazione delle strutture di degenza e dei servizi di supporto che li compongono;
- il sistema delle relazioni funzionali ed operative fra i Dipartimenti ad attività integrata (DAI) dell'Azienda ed i Dipartimenti universitari (DU);
- l'impegno orario di presenza nelle strutture aziendali del personale universitario;
- le modalità di partecipazione del personale del SSR alle attività didattiche;
- le modalità con cui Azienda ed Università concorrono alla promozione ed allo sviluppo della ricerca scientifica e dell'innovazione.

L'Accordo Attuativo Locale, dopo la intesa con la Università, è approvato con specifico provvedimento del Direttore Generale.

Per la formazione specialistica dei laureati in medicina e chirurgia, in applicazione del Protocollo di intesa Regione - Università degli Studi di Bologna, Ferrara, Modena - Reggio Emilia e Parma, sottoscritto il 26 ottobre 2006, si realizza uno specifico Accordo locale fra Azienda ed Università, per disciplinare:

- la partecipazione del personale del S.S.R. alla formazione specialistica;
- la organizzazione della attività formativa;
- la partecipazione dei medici in formazione specialistica alle attività assistenziali;
- le condizioni per la frequenza nelle strutture dell'Azienda.

3. Punti Principali del Documento

Il presente documento contiene idonee informazioni relativamente ai punti dell'art. 19 del Disciplinare tecnico (Allegato B del Codice Privacy) e agli altri punti notevoli della normativa Privacy, come di seguito indicati:

ARGOMENTI	RIFERIMENTO NEL DISCIPLINARE
• L'elenco dei trattamenti di dati personali (Disciplinare tecnico);	19.1
• La distribuzione dei compiti c delle Responsabilità nell'ambito delle strutture	19.2
• L'analisi dei rischi che incombono sui dati;	19.3
• L'indicazione delle misure da adottate e adottande per proteggere le aree e/o i locali ove sono effettuate le operazioni di trattamento;	19.4
• La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati nell`ipotesi di distruzione o danneggiamento	19.5
• La previsione del piano di formazione degli Incaricati del trattamento al momento dell'assunzione, del cambiamento di mansioni, di rilevanti cambiamenti	19.6
• La descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati al1'esterno della struttura dell'Azienda	19.7
• L'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali dell`interessato	19.8
• Le informazioni in ordine alla costituzione del dossier sanitario (linee guida Garante Privacy 16/7/2009)	-
• La descrizione delle misure di sicurezza per il dato cartaceo	-
• La descrizione delle misure di garanzia ai sensi dell'art. 83 Codice Privacy e correlato Provvedimento del 9/11/05 Garante Privacy	-

4. Elenco dei trattamenti di dati personali

4.1. Tipologia dei dati

Nello svolgimento della propria attività istituzionale l'Azienda Ospedaliera tratta le seguenti categorie di dati suddivisi per categoria di riferimento:

4.1.1. Dati Personali

Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, le immagini acquisite ai fini di interventi chirurgici. Nello specifico trattasi di dati relativi a persone fisiche e persone giuridiche in rapporto con l'Azienda Ospedaliera ovvero pazienti, personale dipendente, personale non strutturato (borsisti, collaboratori, tirocinanti), clienti, utenti e fornitori.

4.1.2. Dati sensibili

I dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale. Nello specifico trattasi di dati contenuti nelle cartelle cliniche di ricovero in regime di degenza e day hospital, allegati cartella clinica, informativa e consenso schede ambulatoriali, diari clinici, registri nosologici, registri delle prenotazioni, schede di dimissione ospedaliera, relazioni cliniche, archivi di attività diagnostiche/terapeutiche (impegnative, ricevute di ticket, cartelle ambulatoriali, referti, lastre), registri di sala operatoria, registri dei decessi, registri delle autopsie, registri e documenti relativi alle sperimentazioni cliniche, dati relativi alle donazioni, copia di certificati di richieste documentazione sanitaria accertamenti relativi all`idoneità lavorativa, dati idonei a rivelare il comportamento sessuale, schede personali relative all'iscrizione ai sindacati, curriculum vitae, fascicoli del personale dipendente. Tali dati possono essere trattati anche in forma di rappresentazione grafica, fotocinematografica, elettromagnetica.

4.1.3. Dati Giudiziari

I dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a 0) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli art. 60 e 61 del codice di procedura penale.

4.2. Tipologia dei trattamenti

I dati personali come sopra elencati sono oggetto di trattamento mediante qualunque operazione o complesso di operazioni, effettuati anche senza l'ausi1io di strumenti elettronici e anche se non registrati in una banca di dati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati, anche non registrati in una banca dati. In particolare, l'interconnessione e la comunicazione dei dati può configurarsi con aziende ospedaliere e sanitarie, anagrafe regionale, ministero della salute, Istat, regioni e province autonome, centro nazionale trapianti, istituto superiore sanità, ministero di giustizia, comunicazioni con esercente la potestà, enti previdenziali, autorità giudiziaria, organi di controllo, organizzazioni sindacali, assicurazioni eccetera.

4.3. Dati trattati nell'ambito dell'attività svolta

Nell'ambito dell'attività svolta dalle Aziende Sanitarie vengono trattati i dati specificamente riportati nel Regolamento regionale n. 3 del 24 aprile 2006, approvato dall'Assemblea Legislativa Regionale con delibera n. 53 del 19 aprile 2006.

Tale regolamento identifica, ai sensi dell`art. 20 del D.Lgs. 196/2003, i tipi di dati e le operazioni eseguibili da parte delle Aziende Sanitarie della Regione Emilia-Romagna nello svolgimento delle proprie funzioni istituzionali, con riferimento ai trattamenti di dati sensibili e giudiziari effettuati per il perseguimento delle rilevanti finalità di interesse pubblico individuate da espressa disposizione di legge, ove non siano legislativamente specificati i tipi di dati e le operazioni eseguibili.

L'Azienda svolge inoltre attività connesse a: adempimenti giuridico amministrativi relativi ai rapporti con l'Università degli Studi; adempimenti connessi alla adozione dei provvedimenti del Direttore Generale e di competenza diretta o delegata dei dirigenti di struttura complessa Tecnico Amministrativa; gestione del sistema delle relazioni istituzionali con gli Enti di riferimento; svolgimento delle attività amministrative collegate a talune tipiche funzioni sanitarie; organizzazione dell`attività didattica e valutazione dei bisogni formativi del personale; gestione dei rapporti con i fornitori/creditori; gestione delle procedure connesse all'acquisizione di beni e servizi nel rispetto della normativa comunitaria, nazionale e regolamentare; gestione delle attività economiche di supporto all'attività sanitaria e assistenziale e monitoraggio delle attività appaltate; gestione delle procedure e attività, tecniche e amministrative, connesse alla gestione del patrimonio mobiliare e immobiliare, ivi compreso il controllo delle apparecchiature elettromedicali e le relative verifiche di sicurezza; funzioni per l'adempimento degli obblighi previsti dalla L. 626/1994 e s.i.m..

4.4. Area di trattamento

Le operazioni di trattamento si svolgono presso le strutture di assistenza ospedaliera in regime di degenza, ambulatoriale, day hospital, domiciliare, nonché presso le strutture sanitarie e amministrative di seguito indicate, come da atto aziendale deliberazione Direttore Generale n. 215 del 30/11/2015:

- (Art 21) Servizi e direzioni in staff:
    - Direzione professioni sanitarie (in staff alla Direzione Generale)
    - Comunicazione e Informazione (in staff alla Direzione Generale):
    - Servizio Formazione e Aggiornamento (in staff alla Direzione Generale)
    - Direzione Servizi Ospitalità (in staff alla Direzione Generale)
    - Servizio prevenzione e protezione aziendale (in staff al Direttore Generale)
    - Ricerca e Innovazione (in staff al Direttore Sanitario)
    - Assicurazione Qualità (in staff al Direttore Sanitario)
    - Servizio Sicurezza ed Autorizzazione (in staff al Direttore Sanitario)
    - Progettazione organizzativa (in staff al Direttore Sanitario)

- (Art. 23) Direzioni Tecniche Aziendali. Afferiscono al Direttore sanitario e sono le seguenti:
    - Direzione Assistenza farmaceutica
    - Medicina legale
    - Fisica Medica

- (Art 24) Direzioni Tecnico – Amministrative: Afferiscono al Direttore Amministrativo e sono le seguenti:
    - - Segreteria Generale
    - - Servizio Interaziendale Amministrazione del Personale
    - - Servizio attività amministrative ospedaliere

- - Servizio appalti ed acquisti
- - Servizio attività tecniche e patrimoniali
- - Servizio Bilancio e Finanze
- - Controllo di Gestione
- - Servizio Ingegneria Clinica
- - Servizio Tecnologie dell'Informazione

- (All. C) Diparimenti ad Attività Integrata (DAI), Interaziendali ad attività integrata, Interaziendali
  - DAI 1 - MEDICINE, MEDICINA D'URGENZA E SPECIALITÀ MEDICHE
    a. Medicina I
    b. Medicina Interna e Area Critica (
    c. Gastroenterologia
    d. Malattie Infettive
    e. Reumatologia
    f. Degenza Post Acuzie
    g. Malattie dell'Apparato Respiratorio
    h. Tossicologia Medica – Centro cefalee e abuso di farmaci
    i. Malattie del Metabolismo e Nutrizione Clinica

  - DAI 2 - CHIRURGIA GENERALE E SPECIALITÀ CHIRURGICHE
    a. Chirurgia I
    b. Chirurgia II
    c. Chirurgia Toracica
    d. Urologia
    e. I Servizio Anestesia e Rianimazione
    f. II Servizio Anestesia e Rianimazione
    g. Chirurgia oncologica, epato-bilio-pancreatica e dei trapianti di fegato
    h. Chirurgia Oncologia Senologica

  - DAI 3 - MATERNO-INFANTILE
    a. Ostetricia-Ginecologia
    b. Ginecologia
    c. Pediatria
    d. Chirurgia Pediatrica
    e. Pediatria ad Indirizzo Oncoematologico
    f. Neonatologia e Nido
    g. Genetica Medica
    h. Sviluppo neuropsichiatria infantile

  - DAI 4 - ONCOLOGIA ED EMATOLOGIA
    a. Oncologia
    b. Medicina Oncologica
    c. Ematologia
    d. Radioterapia
    e. Immuno-Trasfusionale
    f. Medicina Nucleare
    g. Terapie Palliative e Hospice
    h. DH Oncologico
    i. Terapie oncoematologiche innovative

- DAI 5 – CHIRURGIE SPECIALISTICHE
  a. Chirurgia Plastica Ricostruttiva
  b. Malattie Oftalmologiche
  c. Odontoiatria e Chirurgia Oro-Maxillo-Facciale
  d. Dermatologia
  e. Otorinolaringoiatria
  f. Ortopedia e Traumatologia
  g. Chirurgia della Mano
  h. Riabilitazione della mano
  i. Chirurgia Cranio - Maxillo Facciale

- DIPARTIMENTO INTERAZIENDALE AD ATTIVITÀ INTEGRATA MALATTIE NEFROLOGICHE, CARDIACHE E VASCOLARI
  a. Cardiologia
  b. Nefrologia e Dialisi
  c. Studio della ipertensione polmonare e cura delle patologie vascolari del piccolo circolo

- DIPARTIMENTO INTERAZIENDALE INTEGRATO DIAGNOSTICA PER IMMAGINI
  a. Radiologia
  b. Radiologia Interventistica

- DIPARTIMENTO INTERAZIENDALE INTEGRATO MEDICINA DI LABORATORIO E ANATOMIA PATOLOGICA
  a. Laboratorio Analisi Chimico-Cliniche
  b. Microbiologia e Virologia
  c. Tossicologia e Farmacologia Clinica
  d. Anatomia ed Istologia Patologica
  e. Diagnostica avanzata delle infezioni fungine

- DIPARTIMENTO INTERAZIENDALE FARMACEUTICO
  a. Farmacia

- DIPARTIMENTO INTERAZIENDALE DI EMERGENZA E URGENZA (D.I.E.U.)
  a. Pronto Soccorso e Medicina d'Urgenza

Le unità operative e i moduli dipartimentali che costituiscono l'organigramma di ciascun Dipartimento ad Attività Integrata sono declinate nei provvedimenti aziendali con cui sono approvati il Regolamento dei Dipartimenti ad Attività Integrata, l`Accordo Attuativo Locale con l'Università degli Studi di Modena e Reggio e i relativi aggiornamenti.

4.5. Elenco dei trattamenti.

Questa sezione riporta l'elenco dei trattamenti di dati personali effettuati dalla Azienda Ospedaliero Universitaria Policlinico di Modena.

I seguenti trattamenti si intendono effettuati sia con strumenti elettronici sia attraverso più tradizionali supporti cartacei (GDPR Art. 30):

- Trattamenti di ambito sanitario generale
    - Attività ambulatoriale
    - Attività di ricovero
    - Soccorso sanitario di emergenza urgenza (118) e assistenza sanitaria di emergenza (PS)

- Trattamenti di ambito sanitario specific
    - Attività ispettive (interne)
    - Servizio Prevenzione e Protezione Aziendale
    - Sorveglianza Sanitaria
    - Fisica Medica
    - Attività immuno - trasfusionale
    - Attività di genetica medica
    - Ricerca
    - Medicina Legale compresa l'attività di gestione del rischio clinico
    - Farmacovigilanza

- Trattamenti di ambito tecnico-amministrativo
    - Gestione contenzioso e ricorsi e attività di tutela amministrativa e giudiziaria, gestione assicurazioni
    - Gestione del patrimonio, Attività contabili
    - Gestione documentale (compreso accesso agli atti)
    - Gestione risorse umane
    - Attività di informazione e comunicazione con l'utenza
    - Gestione sistemi a supporto della attività dei servizi tecnici
    - Attività sistemistica relative alle funzioni di Amministratore di sistema, di rete, di base dati, software e applicazioni
    - Analisi dati e statistiche comprende Epidemiologia e comunicazione del rischio e controllo di gestione
    - Videosorveglianza

In Appendice A l'elenco degli applicativi suddiviso per incaricati al trattamento

5. La distribuzione dei compiti e delle responsabilità

Il documento deve essere conosciuto ed applicato dal Titolare, dai Responsabili e dagli Incaricati, secondo le competenze di seguito descritte:

5.1. Il Titolare del trattamento

E' l'ente nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati è l'Azienda Ospedaliero - Universitaria di Modena nella persona del suo Rappresentante Legale, cui competono le decisioni in ordine alle finalità e modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza. Il Titolare del trattamento individua per iscritto i Responsabili del trattamento dei dati ed affida loro, per quanto di competenza, il compito di porre in essere ogni misura tesa a ridurre al minimo i rischi di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite con ogni mezzo ritenuto più idoneo.

5.2.I Responsabili del trattamento

Nell'ambito del Regolamento recante il sistema di gestione dei dati personali all'interno dell'Azienda Ospedaliero-Universitaria di Modena in applicazione dcl decreto legislativo 196/2003 (Codice Privacy), approvato con deliberazione n. 90 del 10.5.2007, l'Azienda ospedaliera ha esercitato la facoltà di nomina dei Responsabili ai sensi dell'art. 29, primo comma, e ha individuato gli stessi fra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza (articolo 5 del Regolamento).

In particolare, sono stati designati quali Responsabili i Dirigenti Responsabili di struttura complessa Ospedaliera e Universitaria, di struttura semplice dipartimentale, di programma assistenziale per quanto riguarda le Unità Operative/Servizi Sanitari, e i Dirigenti Responsabili di struttura complessa, i Responsabili di struttura semplice e delle unità organizzative/strutture di staff per quanto riguarda le funzioni tecnico amministrative e di staff, i cui compiti sono stati analiticamente specificati per iscritto dal Titolare. Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui sopra e delle proprie istruzioni.

Il trattamento dati in regime di outsourcing è disciplinato da apposite procedure.

5.3.Gli Incaricati al trattamento

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

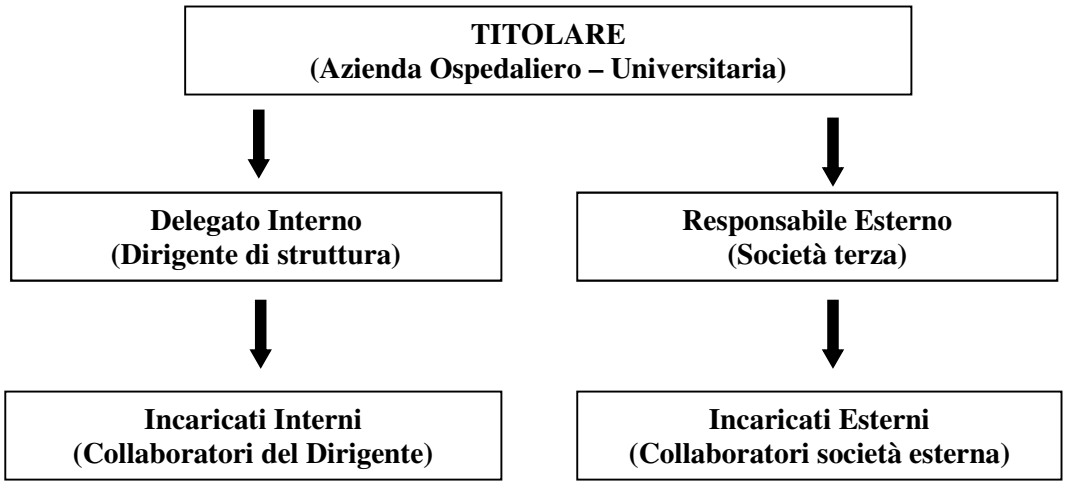
L'Azienda ospedaliera ha adempiuto all'obbligo di nomina ai sensi dell'art. 30, mediante designazione effettuata per iscritto nell'ambito del Regolamento recante il sistema di gestione dei dati personali all'interno dell'Azienda Ospedaliero-Universitaria di Modena in applicazione del decreto legislativo 196/2003 (Codice Privacy), approvato con deliberazione del 14/08/2015 e individuazione puntuale dell'ambito del trattamento consentito.

Si può considerare tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Nella modulistica utilizzata per richiedere le credenziali di autenticazione ai sistemi informatici aziendali si evidenzia che l'accoglimento della richiesta e la creazione di un profilo di autenticazione notificato al richiedente coincide "de facto" con la nomina ad incaricato al trattamento, impartendo, anche attraverso rimandi alla intranet aziendale, tutte le opportune istruzioni.

Gli incaricati ricevono un'adeguata formazione tecnico - giuridica. In definitiva si configura il seguente modello organizzativo:

ORGANIGRAMMA PRIVACY



5.4. Amministratori di Sistema

In ottemperanza alle prescrizioni del Garante per la Protezione dei dati personali contenute nel Provvedimento 27.11.2008, successivamente modificato con Provvedimento 25.6.2009, il Responsabile del Sistema informatico, del quale sono state individuati funzioni e responsabilità nel Regolamento aziendale recante il sistema di gestione dei dati personali all'interno dell'Azienda Ospedaliero-Universitaria di Modena, ha individuato quale amministratore di sistema tutto il personale del Servizio Tecnologie dell'Informazione, ciascuno con riferimento e nei limiti delle effettive mansioni svolte.

6. Analisi dei rischi

I principali rischi presi a riferimento per la adozione delle misure di sicurezza esplicitate nel presente documento sono così riassumibili :

1. si considerano gravi le minacce che possono limitare e/o rendere difficoltosa l'erogazione della attività assistenziale;
2. si considerano gravi le minacce che portano alla divulgazione/modifica/produzione illegittima di dati sensibili o che comportino un danno patrimoniale per l'azienda;

In particolare:

3. si considerano gravi le minacce che possono limitare la disponibilità di servizi informatici a supporto delle attività assistenziali;
4. si considerano gravi le minacce che portano alla modifica illecita di messaggi – e quindi di informazioni gestite dall'azienda - qualora tali messaggi abbiano un valore medico-legale o la loro modifica comporti un danno patrimoniale per l'azienda;
5. si considerano gravi le minacce di fraudolenta impersonificazione – masquerade – qualora ciò porti alla produzione di falsi atti con valore medicolegale o che comportino un danno patrimoniale per l'azienda;

6. si considerano gravi le minacce di fraudolenta impersonificazione – masquerade – qualora ciò porti alla modifica fraudolenta di atti con valore medico-legale originariamente legittimi, o qualora ciò porti ad un danno patrimoniale per l'azienda;
7. si considerano gravi le minacce di intercettazione qualora i dati intercettabili riguardino dati personali di natura sensibile ai sensi della legge sulla tutela dei dati personali.

Si considerano in genere trascurabili le minacce di analisi del traffico e di ripetizione, a patto che esse non portino a conseguenze elencate nei punti sopra elencati.

7. Misure per la Sicurezza Informatica

7.1.Sicurezza Fisica dei Dati

Al fine di garantire la sicurezza dei dati dal punto di vista fisico, sono stati adottati alcuni provvedimenti, di seguito descritti:

7.1.1. Locali Server

Tutti i server sono posizionati in locali chiusi il cui accesso è consentito esclusivamente alle persone autorizzate.

Tali locali sono dotati di condizionatori d'aria che garantiscono la corretta temperatura di funzionamento.

Sono installati due tipologie di condizionatori d'aria che garantiscono la temperatura ottimale anche in caso di guasto di una delle due tipologie.

7.1.2. Raffreddamento Interno dei Server

Tutti i Cabinet dei server sono dotati di ventole di raffreddamento aggiuntive e ridondanti che garantiscono un ottimo ricambio d'aria all'interno dello stesso in modo da evitare pericolosi surriscaldamenti delle componenti interne.

Tutti gli HDs sono raffreddati anche da una ventola posizionata opportunatamente per mantenere la temperatura degli stessi uguale a quella ambientale e quindi, anche nella peggiore delle ipotesi, entro i limiti di sicurezza stabiliti dal costruttore. i.e. la temperatura dell'aria a contatto con gli HDs < = 50°.

7.1.3. Protezione Elettrica

Tutti i Server sono protetti da qualsiasi problema a carico dell'energia elettrica con un gruppo di continuità (UPS) del tipo on-line, doppia conversione, che garantisce un perfetto funzionamento del sistema in caso di microinterruzioni o elevati picchi di tensione (anche di migliaia di Volts) che si possono presentare sulla linea elettrica di alimentazione.

La qualità della corrente erogata è conforme allo standard, i.e. forma d'onda con THD < 3% assicurata in qualsiasi condizione.

In caso di Blackout inferiori a 5 min, l'UPS assicura il perfetto funzionamento del Server, nel caso di Blackout superiori ai 5 min, il Sw di gestione dell'UPS provvede autonomamente a spegnere correttamente il Server.

Allo stesso modo il Sw provvede autonomamente alla riaccensione del server quando la condizione di Blackout viene a cessare.

7.1.4. Configurazione dei dischi

La casistica dimostra che le parti meccaniche sono quelle più soggette a rottura e quindi gli HDs sono i dispositivi meccanici contenenti Dati che devono essere oggetto di maggior attenzione.

Il caso più frequente, statisticamente parlando, è la rottura fisica degli HDs che comporta la perdita totale dei dati memorizzati sul supporto.

Per fornire una sostanziale protezione da tali rischi, tutti i Server hanno i dischi configurati in Mirror Mode o Stripe-Set Mode.

7.1.5. Salvataggi giornalieri su disco di backup

Tutti i Server effettuano giornalmente un salvataggio dei dati su un apposito HD di Backup in modo Full il

giorno 1 di ogni mese, in modo Incremental tutti gli altri giorni; tale implementazione è attiva su TUTTI i server.

La prima copia su un server dedicato di Backup nello stesso building del server, poi la notte stessa il server si sincronizza con un server simile situato in un Building diverso per garantire il disaster Recovery

7.1.6. Nodi di rete

Tutti i nodi della rete sono situati in armadi metallici dotati di serratura e di sistema di raffreddamento tramite ventole. L'accesso a tali nodi è consentito esclusivamente alle persone autorizzate.

7.2.Sicurezza logica dei dati

7.2.1. Sistema di Autenticazione

Il trattamento di dati personali è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata, conosciuta solamente dal medesimo.

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

Agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato. (D. Lgs. 196/2003 Allegato B, paragrafi 1-2-3-4)

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Pertanto si dispone che ogni utente definito non venga più cancellato, ma disabilitato nel caso cessi di essere in uso, in maniera tale da evitarne il riutilizzo. (D. Lgs. 196/2003 Allegato B, paragrafo 6).

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri, oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni tre mesi.

. Qualora il sistema operativo dell'elaboratore su cui risiede l'applicativo lo consenta, è abilitato il cambio password, che l'incaricato potrà autonomamente effettuare in un qualsiasi momento successivo al primo accesso, e in ogni altro momento successivo; per quei sistemi operativi per i quali non sia disponibile tale modalità di cambio password, o non sia comunque abilitabile per ragioni tecniche, l'incaricato potrà avvalersi della consulenza del personale del Servizio Tecnologie dell'Informazione (STI), per individuare la modalità tecnico/organizzativa più idonea allo scopo.

(D. Lgs. 196/2003 Allegato B, paragrafo 5)

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della

componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato. (D. Lgs. 196/2003 Allegato B, paragrafi 7-8-9-10)

7.2.2. Altre misure di Sicurezza

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

I dati personali sono protetti contro il rischio di intrusione da programmi di cui all'art. 615quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

Gli aggiornamenti periodici dei programmi per elaboratore, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti, sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. (D. Lgs. 196/2003 Allegato B, paragrafi 15-16-20-17-18) E' vietato il reimpiego dei supporti di memorizzazione qualora essi siano serviti per la memorizzazione di dati personali o sensibili. È inoltre genericamente vietato l'utilizzo di supporti di memorizzazione rimovibili per lo scambio di dati sensibili. (D. Lgs. 196/2003 Allegato B, paragrafi 21 e 22)

Fanno eccezione a questa politica i supporti di memorizzazione impiegati per i backup dei server, che vengono ciclicamente reimpiegati, fino al momento in cui diventano inservibili e vengono fisicamente distrutti.

Per quanto attiene agli adempimenti relativi a quanto prescritto nell'art. 22, co. 63 del D. Lgs. 196/2003:

- tutti i nuovi applicativi che vengono acquisiti dall'Azienda, destinati a trattare dati sensibili, devono essere conformi almeno ai requisiti minimi; allo stesso modo, tutte le installazioni effettuate devono essere condotte nel rispetto della vigente normativa;
- il meccanismo di sicurezza che di norma viene utilizzato dai fornitori di soluzioni applicative è la separazione fra dati anagrafici e dati sensibili, in tutti quei casi in cui ciò sia materialmente e tecnicamente possibile; si rimanda comunque alle dichiarazioni dei fornitori al riguardo;
- l'architettura del sistema informativo aziendale viene progettata e realizzata per far sì che un utente del sistema informativo aziendale non possa, con le proprie credenziali applicative, accedere direttamente ai dati contenuti nelle banche dati aggirando i vincoli applicativi;
- esistono eccezioni a questa regola generale, ad esempio gli amministratori delle banche dati – comunemente chiamati Data Base Administrator o DBA – possono accedere, al bisogno, alle banche dati in chiaro, essendo propria della loro mansione la ricerca dei guasti e il controllo a basso livello delle funzionalità applicative;
- comunque sui database server sono attivate le funzionalità di tracciatura degli accessi; pertanto, chiunque acceda alla banca dati deve poter giustificare il proprio operato in base a logiche di necessità ed essenzialità;

- per quanto tecnicamente possibile i percorsi dei dati in rete sono mantenuti localizzati su tratti di rete ad accesso controllato, in maniera tale da minimizzare i pericoli di intercettazione delle informazioni;
- per poter gestire l'erogazione delle prestazioni sanitarie, in modo da garantire ai pazienti una sempre maggiore efficienza ed efficacia nelle cure prestate, è stato realizzato in SIO un sistema di gestione dei precedenti sanitari denominato "Dossier sanitario", al quale i professionisti sanitari possono accedere solamente per finalità di prevenzione, diagnosi, cura, riabilitazione dei pazienti e solamente per il periodo di tempo in cui si articola la presa in carico degli stessi. L'accesso alle informazioni contenute nel Dossier presuppone sempre la previa acquisizione del consenso del paziente in carico; tale consenso è di duplice livello: alla costituzione del Dossier e alla consultazione dei dati contenuti nel suo Dossier e consenso sarà a breve acquisito in maniera informatizzata attraverso un apposito modulo. Naturalmente, il buon uso delle informazioni contenute nel Dossier, oltre che regolamentato da specifico documento aziendale in materia e dalla attività di formazione del personale interessato, è rimesso ad un utilizzo corretto del sistema da parte degli utenti aziendali abilitati, i cui accessi sono comunque soggetti a verifiche e controlli.

È responsabile della formulazione di opportune politiche di gestione dei sistemi di elaborazione che garantiscano il rispetto delle misure minime di sicurezza e della attuazione delle misure attuative, per la parte di competenza, il Servizio Tecnologie dell'Informazione Aziendale.

7.2.3. Antivirus

Tutti i Server e I Client sono dotati di Antivirus con aggiornamento automatico centralizzato.

Il Server di Mail è dotato di apposito Antivirus SMPT che permette un controllo accurato di quanto viene ricevuto e spedito anche nei confronti degli allegati.

Esiste un Front-End SMTP per proteggere il mail server interno, gestire la sicurezza perimetrale e il filtraggio dello spam in arrivo.

7.2.4. Attivazione delle prese di rete

L'attivazione di una presa di viene effettuata esclusivamente su presentazione di una richiesta scritta del responsabile della Unità Operativa interessata indirizzata al Responsabile della Sicurezza Informatica.

Le porte non utilizzate vengono, dove gli apparati lo consentono, disattivate.

7.2.5. Connessione a Internet

La connessione ad Internet avviene tramite collegamento con la rete regionale Lepida S.p.a. che si configura anche come Internet Provider per l'Azienda Ospedaliero – Universitaria di Modena.

Sono presenti, per la protezione perimetrale da Internet:

- Firewall aziendali
- Dmz per i server di frontiera
- Implementazione di NAT e Access List

8. Informazione e Formazione

8.1.Formazione sugli aspetti generali della normativa privacy

In ottemperanza alla regola 19.6 del Disciplinare tecnico (Allegato B al Codice Privacy), si prevedono interventi formativi degli Incaricati del trattamento, per renderli consapevoli dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle Responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal Titolare.

Programma Formativo

Tema	Argomenti
Principi Generali	• Finalità • Principio di Necessità • Definizioni principali • Modalità di Trattamento • Informativa • Consenso • Modalità semplificate • Eccezioni
Soggetti attivi del trattamento	• Titolare • Responsabile • Incaricato
Obblighi di sicurezza	• Misure di sicurezza per il dato cartaceo • Misure di sicurezza per il dato informatico • Altre misure di sicurezza
Responsabilità	• Amministrativa • Penale • Civile

Per tale attività sono state predisposte apposite slides formative.

Il Regolamento recante il sistema di gestione dei dati personali all'intemo dell"Azienda Ospedaliero-Universitaria di Modena in applicazione del decreto legislativo 196/2003 (Codice Privacy) approvato con deliberazione n. 90 del l0.5.2007 individua altresì procedure per tutti gli incaricati/responsabili, relative al trattamento dei dati, al trattamento con strumenti elettronici, al trattamento dei dati genetici, linee guida per

studenti, ecc.

Va inoltre precisato che il Referente aziendale privacy svolge una costante attività di "formazione sul campo", effettuando accessi o riunioni con le singole strutture qualora si rendesse necessario ampliare o approfondire specifiche tematiche sulla materia.

8.2. Informativa/Regole per l'utente

8.2.1. Identificativo di Accesso e Password

Al momento della consegna l'utente dovrà essere informato sul corretto uso del Suo accesso Personale.

La Password è **strettamente segreta** ed è **assolutamente vietato** comunicarla per qualsiasi motivo ad un altro utente, se ciò venisse fatto l'Utente "detentore" della Password risponderà sempre e comunque in prima persona dell'eventuale errato utilizzo del proprio accesso personale sia da un punto civile che penale.

8.2.2. Regole Generali sull'uso del computer aziendale

Contemporaneamente alla consegna dell'ID e Password l'Utente dovrà essere informato sul corretto utilizzo delle attrezzature (in questo caso PC) dell'Azienda Ospedaliero universitaria di Modena, di seguito sommariamente elencate:

- Il PC può essere utilizzato esclusivamente per motivi Aziendali come da incarico ricevuto.
- Tutti i documenti che vengono creati non possono risiedere sul Pc stesso ma devono obbligatoriamente essere salvati su un Server apposito il cui accesso viene dato ad ogni utente che per motivi Aziendali ne abbia necessità come precedentemente accennato.
- E' vietato modificare in qualsiasi modo la configurazione del Pc.
- E' vietato caricare programmi di qualsiasi tipo.
- E' vietato scollegare e/o ricollegare il Pc dalla rete.

Le attività dei tre punti precedenti queste possono essere svolte solo dal Personale del S.T.I. o da personale espressamente autorizzato dal S.T.I. stesso.

8.2.3. Internet e Posta Elettronica

Nei paragrafi seguenti vengono richiamate alcune indicazioni di buona gestione del sistema informativo aziendale e delle attrezzature aziendali. Le indicazioni riportate devono essere integrate da quanto riportato nell'Allegato A, denominato "Disciplinare per l'utilizzo delle postazioni di lavoro dell'Azienda Ospedaliero – Universitaria di Modena" (c.d. Disciplinare).
Tali regole informano gli incaricati e forniscono indicazioni cogenti in ottemperanza a quanto prescritto dal provvedimento del Garante per la Protezione dei Dati Personali "Lavoro: le linee guida del Garante per posta elettronica e internet" in (G.U. n. 58 del 10 marzo 2007). Il suddetto disciplinare viene emanato ai sensi di quanto previsto al punto 3.2 del dette linee guida.

8.2.4. Crimine informatico e tutela del diritto d'autore

È compito del Servizio Tecnologie dell'Informazione Aziendale informare il personale aziendale al buon uso del sistema informatico e telematico aziendale, al fine di prevenire il crimine informatico; ad ogni corso di formazione sull'utilizzo di applicativi in uso in Azienda il discente viene sistematicamente informato sulla normativa relativa al crimine informatico. Gli appartenenti al Servizio STI Aziendale sono informati su quanto prevede la vigente normativa in materia di crimine informatico – legge n. 547 del 23/12/1993.

Il Servizio ICT Aziendale, qualora tecnicamente possibile, predispone copie di riserva dei programmi dotati di regolare licenza, allo scopo di prevenire accidentali perdite dell'originale e quindi danni patrimoniali all'Azienda. Tale copia di riserva potrà essere usata soltanto per ripristinare le funzionalità del programma, quando non sia possibile utilizzare il programma originale.

8.2.5. Virus Informatici – Malware

Al fine di prevenire le infezioni virali si adottano le seguenti misure:

1. si dotano tutte le attrezzature di confine di un adeguato software antivirale e si stabilisce l'aggiornamento delle firme almeno in ragione giornaliera;
2. si dota di software antivirale ogni nuovo client acquistato e si predispongono adeguati meccanismi per mantenere tale software aggiornato;
3. ogni stazione di lavoro personale dotata di memorie di massa removibili – lettore di floppy disk e similari – che abbia strumenti di produttività personale e che mantenga documenti in locale, o che abbia configurato un client di posta elettronica, deve essere dotata di software antivirale;
4. per quanto possibile si dovranno configurare i profili abilitativi di tutti gli utenti aziendali con privilegi che non consentano l'installazione o l'esecuzione di programmi non autorizzati, sia sulle macchine client, che sui server;
5. per quanto organizzativamente possibile ed appropriato, dovranno essere disabilitate sui server le funzionalità di editor e di file transfer.

Almeno in ragione mensile si effettua una ricognizione sul livello di aggiornamento del software presente sulle attrezzature di confine e sui server al fine di verificare se sia necessaria l'installazione di eventuali FIX e/o effettuare modifiche di configurazione, al fine di aumentare il grado di sicurezza delle stesse: la valutazione se operare o meno delle modifiche alle configurazioni o degli aggiornamenti software andrà fatta ogni volta valutando costi e benefici di dette operazioni.

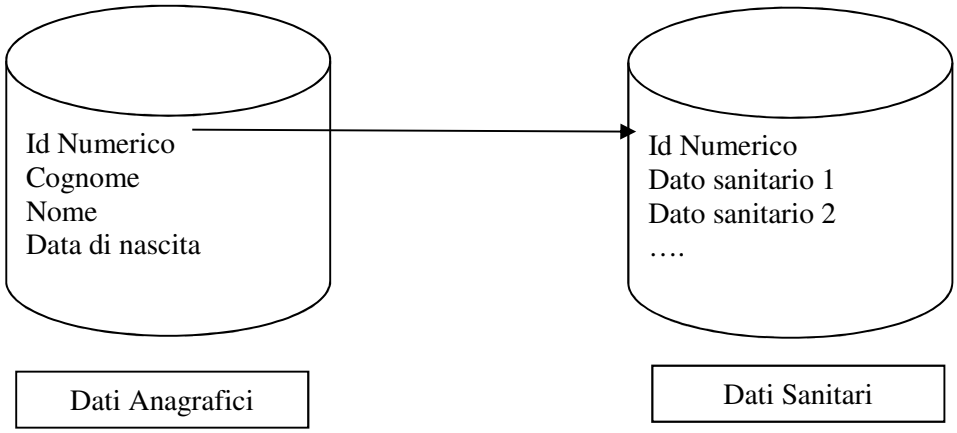
9. Trattamenti affidati all'esterno (outsourcing)

In base a determinate esigenze aziendali, l'Azienda ha affidato il trattamento dei dati in tutto o in parte a soggetti terzi in modalità outsourcing, l'Azienda ha altresì provveduto a nominare formalmente, per iscritto, tali soggetti quali Responsabili del trattamento dei dati ai sensi e per gli effetti della vigente normativa. Conseguentemente, ai suddetti Responsabili del trattamento in modalità outsourcing dovranno ascriversi gli obblighi ed oneri legislativamente previsti circa il trattamento dei dati nonché la legittimazione passiva nell'ipotesi di violazione delle predette disposizioni. Il Responsabile del trattamento deve, tra l'altro:

- garantire il pieno rispetto delle vigenti disposizioni legislative in materia di trattamento, compreso il profilo relativo alla sicurezza, e le connesse procedure aziendali da parte degli incaricati;
- attenersi alle istruzioni impartite dal titolare il quale, anche tramite verifiche ispettive periodiche, vigila sulla puntuale osservanza delle proprie istruzioni;
- non effettuare in alcun modo trattamenti autonomi di dati raccolti e trattati in qualità di Responsabile;
- provvedere alla nomina dei propri collaboratori quali incaricati del trattamento dati e definire l'ambito di trattamento dati al quale gli stessi possono avere accesso;
- consentire al Titolare del trattamento i controlli e la vigilanza sulla corretta osservanza delle disposizioni di legge e delle istruzioni presenti e future impartite;
- valutare e adottare le misure di sicurezza idonee e preventive, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati medesimi, provvedendo, con cadenza almeno semestrale, ad inoltrare al Titolare comunicazione in ordine alle misure di sicurezza adottate;
- segnalare con tempestività al Titolare eventuali problemi relativi all'applicazione della disciplina di cui al D.Lvo. 196/2003 riscontrati nell'esercizio delle attività di competenza.

10. Criteri per la cifratura (o separazione) dei dati

L'architettura del software applicativo dell'azienda ospedaliero universitaria di Modena risponde al modello di anagrafe unica centralizzata ed eventualmente propagata su più server all'interno del campus
Il concetto di anagrafe centralizzata, secondo i principi dei database relazionali si può raffigurare come segue.



Il concetto di anagrafe centralizzata prevede che le diverse tabelle fisiche contenenti le informazioni siano correlate tra loro attraverso un id numerico univoco.
Solo disponendo di tutte le tabelle correlate è possibile mettere in relazione i dati anagrafici con i dati sanitari.
Per quanto riguarda l'acquisizione di software applicativo eventualmente affidata ad agenzie esterne i criteri adottati prevedono:
In tutti i capitolati di gara riguardanti software che trattano dati sensibili si precisa la necessità di fornire moduli software coerenti con questo modello, salvo ulteriori maggiori cautele (crittografia) da adottare anche in coerenza con l'evoluzione delle tecnologie
Nella stipula o nel rinnovo di contratti di manutenzione di software applicativi che trattano dati sensibili si acquisisce dalle agenzie esterne implicate l'impegno contrattuale ad eseguire le manutenzioni software in coerenza con il modello sopra esplicitato.

11. Misure per il trattamento dei dati cartacei

Il Titolare del trattamento ha predisposto le seguenti istruzioni operative finalizzate a ridurre il rischio privacy nell'ipotesi di trattamento di dati sensibili su supporto cartaceo:

- i documenti e gli atti contenenti dati personali devono essere custoditi dagli incaricati in modo tale che non siano accessibili a soggetti non autorizzati e al termine di ogni operazione di trattamento, i documenti e gli atti contenti dati personali e sensibili devono essere riposti all'interno di un luogo sicuro accessibile ai soli soggetti autorizzati;
- per il periodo in cui i documenti sono all'esterno del luogo sicuro vanno osservate tutte le misure di sicurezza, ed in particolare le istruzioni particolareggiate per l'invio o la spedizione all'esterno della struttura dei documenti e degli atti contenti dati personali e/o sensibili;
- va prestata la massima attenzione ai documenti costituiti da fascicoli o raccoglitori. L'incaricato deve sempre accertarsi che le pagine siano complete, verificando il numero e l'integrità dei fogli; al termine dell'orario di lavoro i documenti contenenti dati personali e sensibili non vanno mai abbandonati sulla scrivania o lasciati incustoditi;
- al termine delle operazioni di trattamento occorre sempre riposizionare i documenti all'interno del luogo sicuro individuato al punto precedente. Nel caso in cui non sia possibile riposizionare i documenti all'interno dell'archivio generale, l`incaricato dovrà individuare un luogo di sicurezza temporanea, preventivamente identificato e sottoposto a procedure di sicurezza minima (cassaforte, armadio di sicurezza, classificatore ad accesso controllato, ecc);
- la distribuzione di chiavi per l'accesso ai luoghi sicuri (archivio generale 0 temporaneo) va effettuata sempre in maniera controllata;
- se l'incaricato è costretto ad allontanarsi momentaneamente non deve mai lasciare incustoditi i documenti e gli atti contenenti dati personali e sensibili sulle scrivanie o in altro luogo liberamente accessibile a terzi non autorizzati; si deve limitare all'indispensabile la duplicazione (fotocopie, lanci di stampa, riproduzioni, ecc) di documenti e degli atti contenti dati personali e sensibili;
- ogni consegna di atti e documenti deve sempre avvenire nel rigoroso rispetto di misure minime di sicurezza. In particolare, la consegna di atti e documenti contenenti dati personali e/o sensibili dovrà sempre avvenire in busta chiusa e sigillabile, o effettuata personalmente ai soggetti Interessati, al fine di ridurre al minimo la possibilità che soggetti terzi non autorizzati possano venire a conoscenza del contenuto;
- indipendentemente dal tipo di spedizione adottato è opportuno sempre accertarsi, personalmente quando possibile, che il destinatario abbia effettivamente ricevuto la documentazione inviata;
- non riutilizzare mai le fotocopie di documenti contenti dati personali e/o sensibili come carta riciclata.

12. Dossier sanitario

Nel quadro del processo di ammodernamento della sanità, questa Azienda intende migliorare la propria efficienza nella qualità delle cure e dell'assistenza, assicurando la disponibilità immediata di dati sempre completi cd aggiornati, e quindi offrire un servizio più efficiente ed efficace agli assistiti.

E' indispensabile, per le finalità di prevenzione, diagnosi, cura e riabilitazione, disporre di un quadro il più possibile completo delle informazioni sanitarie che riguardano ciascun interessato; una conoscenza approfondita dei dati clinici, relativi anche al passato, può contribuire ad una più efficace ricognizione degli elementi utili alla valutazione del caso.

Ciò avviene attraverso la creazione di un dossier sanitario, inteso come insieme di dati sanitari riportati in uno o più documenti elettronici tra loro collegati, condivisibili, nell'ambito dei principi di liceità, necessità, pertinenza e non eccedenza, dai sanitari e dai soggetti incaricati del trattamento dal Titolare, e trattati quando ciò sia strettamente necessario al perseguimento delle finalità clinico-assistenziali.

E' garantito all`interessato l`oscuramento di un singolo evento o la revoca del consenso al dossier sanitario.

Il mancato consenso, totale o parziale, alla costituzione del dossier sanitario non incide sulla possibilità di accedere alle cure mediche.

L'Azienda Ospedaliero-Universitaria di Modena, nel costituire il dossier rispetta le "Linee guida in tema di Fascicolo sanitario elettronico e di Dossier sanitario" adottate dal Garante per la protezione dei dati personali il 16.7.2009 e pubblicate nella G.U. n. 178 del 3.8.2009, nonché le disposizioni normative a tutela dell'anonimato della persona tra cui quelle a tutela delle vittime di atti di violenza sessuale o di pedofilia (1. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269 e l. 6 febbraio 2006, n. 38), delle persone sieropositive (1. 5 giugno 1990, n. 135), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (d.P.R. 9 ottobre 1990, n. 309), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (1. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349), nonché con riferimento ai servizi offerti dai consultori familiari (l. 29 luglio 1975, n. 405). Pertanto, tali informazioni non verranno inserite nel dossier, ovvero potranno essere inserite a fronte di una Sua specifica manifestazione di volontà.

Il dossier sanitario potrà essere consultato soltanto da soggetti incaricati del Trattamento da parte dell'Azienda ai sensi del proprio Regolamento aziendale per la gestione dei dati personali, quando ciò sia strettamente necessario al perseguimento delle finalità clinico assistenziali. Potrà essere altresì consultato, nel rispetto dell'autorizzazione generale del Garante, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività (art. 76 Codice Privacy e Autorizzazione generale del Garante n. 2/2009).

13. Misure di garanzia

In ottemperanza all'art. 83 Codice Privacy e al Provvedimento dell`Autorità Garante del 9 novembre 2005, il Titolare del trattamento prevede le misure organizzative, di carattere supplementare rispetto alle misure di sicurezza previste nei punti precedenti, finalizzate a garantire il più ampio rispetto dei diritti e delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale:

13.1. Dignità dell'Interessato

La prestazione medica e ogni operazione di trattamento dei dati personali deve avvenire nel pieno rispetto della dignità dell'Interessato, dignità che deve essere garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria, con particolare riguardo a fasce deboli quali i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno.

Particolare riguardo deve essere prestato nel rispettare la dignità di pazienti sottoposti a trattamenti medici invasivi o nei cui confronti è comunque doverosa una particolare attenzione anche per effetto di specifici obblighi di legge o di regolamento o della normativa comunitaria. Nei reparti di rianimazione dove si possono visitare i degenti solo attraverso vetrate o videoterminali devono essere adottati accorgimenti, anche provvisori che delimitino la visibilità dell'interessato durante l'orario di visita ai soli familiari e conoscenti. In relazione alle modalità di visita e di intervento sanitario effettuati alla presenza di studenti autorizzati, occorre informare il paziente che in occasione di alcune prestazioni sanitarie si perseguono anche finalità didattiche, oltre che di cura e prevenzione.

Inoltre, durante tali prestazioni, devono essere adottate specifiche cautele volte a limitare l'eventuale disagio dei pazienti, anche in relazione alla tipologia di trattamento mediante la limitazione del numero degli studenti presenti e rispettando eventuali legittime volontà contrarie del paziente stesso.

E' stato predisposto il documento recante le linee guida che gli studenti devono rispettare nell'accedere alle strutture ospedaliere.

13.2. Riservatezza nei colloqui e nelle prestazioni sanitarie

É doveroso adottare idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario per evitare che in tali occasioni le informazioni sulla salute dell'Interessato possano essere conosciute da terzi. Le medesime cautele vanno adottate nei casi di raccolta della documentazione di anamnesi, qualora avvenga in situazioni di promiscuità derivanti dai locali o dalle modalità utilizzate. Il rispetto di questa garanzia non ostacola la possibilità di utilizzare determinate aree per più prestazioni contemporanee, quando tale modalità risponde all'esigenza terapeutica di diminuire l'impatto psicologico dell' intervento medico.

13.3. Notizie su prestazioni di pronto soccorso

E' consentito dare notizia, anche per via telefonica, circa una prestazione di pronto soccorso, ovvero darne conferma a seguito di richiesta anche per via telefonica. La notizia o la conferma devono essere però fomite correttamente ai soli terzi legittimati, quali possono essere familiari, parenti o conviventi, valutate le diverse circostanze del caso.

Questo genere di informazioni riguarda solo la circostanza che è in atto o si è svolta una prestazione di pronto soccorso, e non attiene ad informazioni più dettagliate sullo stato di salute.

L'Interessato - se cosciente e capace - deve essere preventivamente informato dall'organismo sanitario e posto in condizione di fornire indicazioni circa i soggetti che possono essere informati della prestazione di pronto soccorso. Occorre altresì rispettare eventuali sue indicazioni specifiche o contrarie.

Il personale Incaricato deve accertare l'identità dei terzi legittimati a ricevere la predetta notizia o conferma, avvalendosi anche di elementi desunti dall`Interessato.

13.4. Dislocazione dei pazienti nei reparti

Il Codice incentiva le strutture sanitarie a prevedere, in conformità agli ordinamenti interni, le modalità per fornire informazioni ai terzi legittimati circa la dislocazione dei degenti nei reparti, allorché si debba ad esempio rispondere a richieste di familiari e parenti, conoscenti e personale del volontariato.

L'Interessato cosciente e capace deve essere, anche in questo caso, informato e posto in condizione all'atto del ricovero di fornire indicazioni circa i soggetti che possono venire a conoscenza del ricovero e del reparto di degenza. Occorre altresì rispettare l'eventuale sua richiesta che la presenza nella struttura sanitaria non sia resa nota neanche ai terzi legittimati. In adempimento a ciò il modulo di consenso prevede che il paziente possa barrare la relativa opzione finalizzata ad un ricovero "in forma anonima". Come per le prestazioni di pronto soccorso, questo genere di informazioni riguarda la sola presenza nel reparto e non anche informazioni sullo stato di salute. Possono essere fornite informazioni sullo stato di salute a soggetti diversi dall'Interessato quando sia stato manifestato un consenso specifico e distinto al riguardo, consenso che può essere anche manifestato da parte di un altro soggetto legittimato, in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'Interessato.

13.5. Distanza di cortesia

Le strutture sanitarie devono predisporre apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento di dati sanitari nel rispetto dei canoni di confidenzialità e della riservatezza dell'Interessato.

Devono essere adottate appropriate soluzioni, sensibilizzando gli utenti con idonei inviti, segnali o cartelli.

13.6. Ordine di precedenza e di chiamata

All'interno dei locali di strutture sanitarie, nell'erogare prestazioni sanitarie o espletando adempimenti amministrativi che richiedono un periodo di attesa devono essere adottate soluzioni che prevedano un ordine di precedenza e di chiamata degli Interessati che prescinda dalla loro individuazione nominativa. Ovviamente, tale misura non deve essere applicata durante i colloqui tra l'Interessato e il personale medico o amministrativo. Quando la prestazione medica può essere pregiudicata in termini di tempestività o efficacia dalla chiamata non nominativa dell'Interessato sono utilizzati altri accorgimenti adeguati ed equivalenti.

Non devono essere affisse le liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta o di intervento effettuato o ancora da erogare. Non devono essere, parimenti, resi facilmente visibili da terzi non legittimati i documenti riepilogativi di condizioni cliniche dell'Interessato.

13.7. Correlazione fra paziente e reparto o struttura

Gli organismi sanitari devono mettere in atto specifiche procedure, anche di formazione del personale, per prevenire che soggetti estranei possano evincere in modo esplicito l'esistenza di uno stato di salute del paziente attraverso la semplice correlazione tra la sua identità e l'indicazione della struttura o del reparto presso cui si c recato o è stato ricoverato. Tali cautele devono essere orientate anche alle eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura. Analoghe garanzie devono essere adottate nella spedizione di prodotti: non devono essere indicati, sulla parte esterna del plico postale, informazioni idonee a rivelare l'esistenza di uno stato di salute dell'Interessato.

13.8. Regole di condotta per gli Incaricati

Il titolare del trattamento deve designare quali Incaricati o, eventualmente, Responsabili del trattamento i soggetti che possono accedere ai dati personali trattati nell'erogazione delle prestazioni e dei servizi per svolgere le attività di prevenzione, diagnosi, cura e riabilitazione, nonché quelle amministrative correlate. Fermi restando, in quanto applicabili, gli obblighi in materia di segreto d'ufficio, deve essere previsto che, al

pari del personale medico ed infermieristico, già tenuto al segreto professionale gli altri soggetti che non sono tenuti per legge al segreto professionale siano sottoposti a regole di condotta analoghe.

A tal fine, anche avvalendosi di iniziative di formazione del personale designato, occorre mettere in luce gli obblighi previsti dalla disciplina in materia di protezione dei dati personali con particolare riferimento all'adozione delle predette misure, evidenziando i rischi, soprattutto di accesso non autorizzato, che incombono sui dati idonei a rivelare lo stato di salute e le misure disponibili per prevenire effetti dannosi.

13.9. Comunicazione di dati all'Interessato

Gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'Interessato informazioni sul suo stato di salute solo per il tramite di un medico o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente.

La necessità di rispettare queste modalità andrebbe menzionata nelle istruzioni impartite agli Incaricati del trattamento. Nel caso in cui l'Interessato riceva una comunicazione dalla struttura sanitaria che documenti gli esiti di esami clinici effettuati, l'intermediazione può essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta. Il personale designato deve essere istruito debitamente anche in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'Interessato. In riferimento alle numerose segnalazioni pervenute, va rilevato che le certificazioni rilasciate dai laboratori di analisi o dagli altri organismi sanitari possono essere ritirate anche da persone diverse dai diretti Interessati, purché sulla base di una delega scritta e mediante la consegna delle stesse in busta chiusa.

Appendice A

Nella seguente tabella vengono riportati gli applicativi suddivisi per incaricati al trattamento

Applicativo	Medici	Caposala	Infermieri	Amministrativi	Tecnici	Farmacisti	Tecnici di laboratorio
Auriga/AurigaLT (Gestione erogato/Gestione attività ambulatoriale)	X	X	X	X			
OstetriciaWeb (Cedap) (gestione percorso nascita)	X	X	X				
Pegaso (Gestione cartelle cliniche in reparto)				X			
Time Out (gestione liste di attesa per sale operatorie)	X	X	X	X			
Wake Up (gestione registro operatorio)	X	X	X	X			
Wake Up Planner (pianificazione utilizzo sale operatorie)		X					
HospitalWeb (gestione richieste Anatomia Patologia e Medicina Trasfusionale)	X	X	X	X			
Mod. Pluri Prescr. (Modulo per gestione prescrizioni esami di laboratorio, esami radiologici e visite specialistiche)	X						
InfoClin Web (Cartella ambulatoriale specialistica)							
Arianna Terapie (gestione terapia informatizzata)	X	X	X			X	
Agenda MedsOffice (gestione attività ambulatoriale)	X	X	X				
ADT (gestione Ricoveri/Movimento/Dimissioni pazienti)	X	X	X	X			
Aurora (PS)	X	X	X	X			
Cassa (gestione attività incasso ticket)				X			
CassaNet (gestione attività economica libera professione)				X			
Turni (gestione turni personale preposto)		X					
SicuroWEB (gestione inventario e manutenzione apparecchiature biomediche)					X		
Armonia (gestione attività Servizio Anatomia Patologica)	X			X			X
Rich. farm. e/o econom. (gestione richieste farmaci, dispositivi medici e beni economali)		X					
NFS (gestione magazzini e procedure amministrative contabili)				X	X	X	
AS400: solo per laboratori	X						X
Archiflow (gestione protocollo informatizzato corrispondenza aziendale - gestione redazione e pubblicazione delibere direzione generale - gestione redazione e pubblicazione determine servizi tecnico-amministrativi)				X			

SyncroMed (gestione attività Servizi di Radiodiagnostica e accesso ai referti/immagini)	X	X	X	X			X
CUP-ISES (gestione agende di prenotazione attività ambulatoriale)				X			
Gestore Richieste (GR) (gestione prenotazioni esami diagnostici e visite ambulatoriali)	X	X	X				
Prescrizioni (PSM) (Modulo per gestione prescrizioni esami di laboratorio e farmaci)	X						
WHR (gestione risorse umane)				X			
COM.Net (gestione pazienti afferenti al COM)	X	X	X	X		X	
Ref. Anat. Pat. (Web) (gestione referti Servizi Anatomia Patologica	X						

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero-Universitaria di Modena

ALLEGATO A - DISCIPLINARE SULL'UTILIZZO DELLE POSTAZIONI DI LAVORO DELL'AZIENDA OSPEDALIERO - UNIVERSITARIA DI MODENA

DISCIPLINARE SULL'UTILIZZO DELLE POSTAZIONI DI LAVORO DELL'AZIENDA OSPEDALIERO - UNIVERSITARIA DI MODENA

Sommario

Premessa

Nel pieno rispetto dei diritti e delle libertà fondamentali dei cittadini, della dignità delle persone con particolare riferimento alla riservatezza, all'identità ed alla protezione dei dati personali (art. 2, comma 1, del Testo Unico – D.Lgs. n° 196/2003) l'Azienda Ospedaliero – Universitaria di Modena adotta il presente "Disciplinare sull'utilizzo delle postazioni di lavoro".
La normativa e gli atti di riferimento del presente Regolamento sono i seguenti:
• D.Lgs n°196 del 2003 e successive modificazioni e integrazioni (Codice in materia di Protezione dei dati personali);

• Codice per la amministrazione digitale (D.Lgs n° 82/2005 e s.m.i);
• Documento Programmatico sulla Sicurezza dell'Azienda Ospedaliero – Universitaria di Modena (vigente);
• Provvedimento a carattere generale del Garante per la protezione dei dati personali dell'1/03/2007 ad oggetto: "Lavoro: le linee guida del Garante per posta elettronica e internet", pubblicato in G.U. n° 58 del 10/03/2007;
• Statuto dei lavoratori (L. n° 300/1970);
• Direttiva n° 2 DD 26/05/2009, c.d. "Direttiva Brunetta", del Dipartimento della Funzione Pubblica della Presidenza del Consiglio dei Ministri.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate. Le proposte verranno esaminate dal Servizio Tecnologie dell'Informazione.
Il presente "Disciplinare" è soggetto a revisione con frequenza almeno annuale da parte del Servizio Tecnologie dell'Informazione.

Art. 1 - Oggetto

Il "Disciplinare" ha per finalità di stabilire le norme per l'accesso e l'utilizzo dei seguenti servizi dell'Azienda Ospedaliero - Universitaria di Modena, di seguito denominata "Azienda":
1) Posta elettronica;
2) Rete internet;
3) Computer aziendali; di seguito indicati nel loro complesso come "Servizi Informatici Aziendali" (d'ora in poi S.I.A.).

L'Azienda garantisce che i dati informatizzati da essa gestiti, nonché i sistemi di elaborazione dati e gli strumenti di telecomunicazioni, non saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114, 171 e 184, co. 3, Codice Privacy; artt. 4 e 8, L. 20 maggio 1970, n.300 – Statuto dei Lavoratori), se non nei limiti consentiti dallo Statuto dei Lavoratori, così come modificato dal D. Lgs. 151/2015 [Jobs Act] e comunque previa informativa ai dipendenti interessati.
Il presente "Disciplinare" è rivolto esclusivamente ai dipendenti dell'Azienda e loro equiparati. Nel seguito del presente documento, per semplicità espositiva, si farà riferimento genericamente all'operatore. Tutte le altre figure (ad es. collaboratori esterni, fornitori, ospiti, ecc…), eventualmente autorizzate, saranno oggetto di un separato disciplinare a cura del Servizio Tecnologie dell'Informazione.
I S.I.A. sono regolamentati, oltre che dalle presenti norme, anche da eventuali altri regolamenti per l'accesso a servizi particolari.

Art. 2 - Definizioni

Nel presente "Disciplinare" i termini di seguito elencati hanno le correlate definizioni:
• BLACK-LIST: elenco dei siti non accessibili agli utenti;
• CATENA DI S. ANTONIO: invio di messaggi di posta elettronica che istighino il destinatario a propagare i messaggi ricevuti ad una pluralità di destinatari, senza attinenza con l'attività lavorativa;
• HOSTING: ospitare sui propri server web le pagine di un sito web esclusivamente di soggetti terzi, rendendolo così accessibile da Internet;

• HOUSING: concessione in locazione ad un utente della possibilità di inserire un suo server all'interno dell'infrastruttura IT aziendale;
• INDIRIZZO IP: numero che identifica univocamente un dispositivo collegato ad una rete informatica;
• INTERNET PROVIDER: azienda che fornisce all'Azienda Ospedaliero - Universitaria di Modena il canale di accesso alla rete Internet;
• LOG: registrazione elettronica automatica generata da applicazioni o dispositivi, riguardante informazioni sulle attività eseguite all'interno degli impianti aziendali;
• MAIL SPAMMING: invio massivo di messaggi di posta elettronica non desiderati e diretti ad una pluralità di destinatari, aventi generalmente contenuto commerciale o comunque non attinente l'attività lavorativa;
• POSTAZIONE DI LAVORO: personal computer (PC), o altro idoneo dispositivo, collegabile alla rete aziendale tramite il quale l'utente accede ai servizi;
• SUPPORTO INFORMATICO: qualsiasi componente in grado di conservare stabilmente dati

informatici;
• UTENTE DI POSTA ELETTRONICA: persona autorizzata ad accedere al servizio di posta elettronica;
• UTENTE INTERNET: persona autorizzata ad accedere al servizio “Internet” con l’esclusione dei siti previsti nella “black-list”;
• MALWARE: Programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico, rubare informazioni sensibili o mostrare pubblicità indesiderata.

Art. 3 - Incaricati al trattamento dei dati personali

I S.I.A. sono strumenti di lavoro forniti dall’Azienda, che ne fissa le modalità di utilizzo: gli utenti sono tenuti ad osservarle scrupolosamente.
Gli utenti sono nominati, ai sensi del Testo Unico u.v., “incaricati al trattamento dei dati personali” a cui hanno accesso o che sono trattati mediante i S.I.A..
I dati devono essere trattati limitatamente alle operazioni indispensabili per le finalità per i quali sono stati raccolti e nei limiti delle funzioni degli incaricati, e comunque nel rispetto dei principi di pertinenza e non eccedenza stabiliti dalle norme vigenti.

Art. 4 - Identificazione dell’utente per l’accesso ai servizi e loro utilizzo

L’utilizzo dei S.I.A. richiede, da parte di tutti gli utenti, un codice di identificazione personale (userid) ed una parola chiave segreta (password).
L’Azienda si riserva, a seguito di evoluzione delle tecnologie, di introdurre, anche solo in particolari contesti, sistemi di autenticazione “forte”, basati, ad esempio, su smart card o caratteristiche biometriche, nel rispetto delle normative vigenti.
Per accedere ai S.I.A., un nuovo utente dovrà fornire i propri dati identificativi, prendere visione del presente regolamento e compilare e sottoscrivere in forma completa in ogni sua parte i moduli di richiesta di abilitazione di volta in volta predisposti e disponibili sulla intranet aziendale (http://intranet.policlinico.mo.it).
Il modulo dovrà essere consegnato alla struttura aziendale deputata alla creazione degli accessi ai sistemi o servizi di cui si richiede l’abilitazione, timbrato e firmato in modo leggibile dal responsabile della struttura organizzativa alla quale l’utente appartiene.
L’incompleta compilazione e autorizzazione del modulo sopra citato, ne comporterà l’automatico annullamento.
L’Azienda si riserva, a seguito di evoluzione della tecnologia, di sostituire la modulistica cartacea con sistemi di autorizzazione elettronica.
La password non potrà essere ceduta a terzi neppure temporaneamente e dovrà essere mantenuta segreta e dovrà essere obbligatoriamente modificata dall’utente in ogni caso in cui egli abbia fondati sospetti che la segretezza della password sia venuta meno.
Qualsiasi azione svolta sotto l’autorizzazione offerta dalla coppia userid e password sarà attribuita in termini di responsabilità all’utente titolare del codice userid, salvo che l’utente dia prova di illecito utilizzo della sua autorizzazione da parte di terzi. L’utente non deve lasciare incustodita o facilmente

accessibile la postazione di lavoro una volta collegata al sistema, e deve disattivare la connessione qualora si debba allontanare. Inoltre non deve rendere accessibili in alcun modo le informazioni concernenti la propria password.
La userid identificativa dell’utente alla cessazione del rapporto di lavoro viene archiviata e non potrà essere riassegnata ad altro utente.
Non sono previsti codici di accesso anonimi, salvo nei casi in cui sia prevista una successiva procedura di identificazione personale per l’accesso alle procedure e/o ai dati veri e propri.
L’utente deve conservare la password con la massima riservatezza e con la massima diligenza.
La password:
• non deve essere banale né contenere riferimenti facilmente riconducibili all’utente;
• dovrà essere lunga almeno 8 caratteri tra i quali: lettere minuscole, lettere maiuscole, numeri, caratteri speciali;
dovrà essere modificata da quest’ultimo al primo utilizzo e successivamente almeno ogni tre mesi.
Alla scadenza dei tre mesi, nel caso in cui l’utente non avesse provveduto a modificare la propria password, l’abilitazione dell’utente verrà sospesa.
L’utente avrà ancora due mesi per riattivare il proprio profilo semplicemente cambiando la password

con le modalità opportune e in modo autonomo.
Alla scadenza di questi ulteriori due mesi, il codice di identificazione personale (userid) verrà disattivato.
Qualora si utilizzino sistemi che non siano in grado di richiedere automaticamente il cambio di password è indispensabile che l'utente – autonomamente - provveda a cambiarla ogni tre mesi.
Nel caso in cui l'utente si dimentichi la propria password, o nel caso in cui l'account venga bloccato a causa di un numero elevato di tentativi d'accesso con una password sbagliata, per riottenere l'accesso ai servizi l'utente dovrà inviare una richiesta di reimpostazione della password al Servizio Tecnologie dell'Informazione (d'ora in poi S.T.I.), firmata e con in allegato una fotocopia del tesserino di riconoscimento aziendale o di un documento di identità valido. Nel caso di disattivazione del codice di identificazione personale per riottenere l'accesso ai servizi l'utente dovrà compilare nuovamente il modulo "Richiesta di abilitazione ai servizi informatici aziendali" e consegnarlo allo S.T.I., firmato dal Responsabile della struttura organizzativa a cui l'utente appartiene.
Dopo sei mesi di non utilizzo dei servizi la userid e la password verranno automaticamente disattivati.
Nel caso in cui l'utente perda la qualità che gli consentiva di accedere ai servizi informatici aziendali, lo S.T.I. a seguito di segnalazione provvederà alla disattivazione di userid e della password.
Nel caso in cui l'utente a seguito di variazione di Servizio o di funzione debba accedere a servizi e/o risorse diverse da quelle previste inizialmente lo S.T.I. a seguito di segnalazione provvederà all'aggiornamento dei privilegi dell'utente.
L'utente si impegna a comunicare immediatamente allo S.T.I. il furto, lo smarrimento, la perdita ovvero l'appropriazione a qualsivoglia titolo da parte di terzi della password.
Nel caso di prolungata assenza dell'utente, egli dovrà utilizzare, qualora siano tecnicamente disponibili, funzioni che consentano di inviare messaggi automatici di risposta per "fuori sede" e che contengano le coordinate per un contatto alternativo con la struttura.
È facoltà del dirigente responsabile dell'utente richiedere allo S.T.I., nel caso di assenze prolungate o improvvise di questi e in condizioni di urgenza e necessità, l'accesso ai suoi dati e messaggi di posta elettronica e consultare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale fatto deve rimanere traccia su apposito verbale informando il lavoratore alla prima occasione utile.
Tenuto conto del provvedimento generale del Garante per la protezione dei dati personali del 01/03/2007 "Lavoro: le linee guida del Garante per la posta elettronica e Internet", relativamente al punto 5.2/b, ove si definisce la figura del fiduciario, si ritiene che i suggerimenti ivi contenuti non siano funzionalmente adottabili dall'Azienda.
Gli strumenti di comunicazione aziendali e gli strumenti di produttività personale in genere – telefono fisso, telefono cellulare, stazioni informatizzate di lavoro, fax, stampanti, ecc… - concessi in uso dovranno essere utilizzati per fini esclusivamente istituzionali e connessi alla propria mansione e attività di servizio. Nessun altro uso di tali strumenti è consentito se non espressamente autorizzato anche se nelle potenzialità della strumentazione concessa in uso ed eventualmente abilitata. A questo proposito è bene precisare che talvolta non è possibile disabilitare determinate funzionalità da alcuni apparati tecnologici, o che questo, anche se tecnicamente possibile, può essere organizzativamente oneroso per l'Azienda; comunque la disponibilità di una determinata

funzionalità non autorizza il consegnatario di un bene all'utilizzo della stessa se non espressamente autorizzato e comunque se non necessario all'espletamento delle proprie mansioni e riconducibile ad attività istituzionali.
Nessun dispositivo personale potrà essere collegato alla rete dell'Azienda e/o utilizzato per trattare dati istituzionali aziendali. Qualora l'Azienda, per l'espletamento della propria attività istituzionale si avvalga di attrezzature la cui gestione in sicurezza ricada sotto la responsabilità di personale non dipendente o a questi assimilabile, dovrà essere formalmente definito un Responsabile esterno che si faccia garante degli aspetti di sicurezza e di rispondenza alla normativa vigente in tema di trattamento dei dati personali per tutti i trattamenti che avvengono su tali attrezzature.
L'Azienda si riserva di verificare l'utilizzo degli strumenti aziendali concessi in uso – ad esempio il telefono, le stazioni di lavoro informatizzate, i palmari, ecc… - qualora si evidenzino volumi anomali di traffico o vi siano altri elementi che indichino un uso non conforme alle presenti indicazioni.
L'Azienda vieta di memorizzare e/o trattare dati a fini personali di qualsiasi tipo per mezzo o all'interno degli strumenti aziendali concessi in uso. Il personale tecnico dell'Azienda, o il personale

delle aziende che in nome e per conto dell'Azienda effettuano attività di manutenzione sugli strumenti aziendali - attrezzature di produttività personale, sistemi di comunicazione, ecc… - potranno accedere a detti strumenti per compiti connessi alla rispettiva funzione e mansione. Non potrà essere addotto come impedimento all'accesso il fatto che siano presenti dati utilizzati a fini personali in forza del suddetto divieto di gestire dati non connessi alla propria mansione e/o attività istituzionale.

Art. 5 - Finalità e limitazioni d'uso

Tenuto conto del provvedimento generale del Garante per la protezione dei dati personali del 01/03/2007 "Lavoro: le linee guida del Garante per la posta elettronica e Internet", l'accesso ai S.I.A. è da intendersi quale "strumento di lavoro".
È pertanto vietato l'uso dei S.I.A. nei seguenti casi:
• per l'utilizzo di procedure aziendali con modalità e finalità non attinenti ai propri doveri d'ufficio;
• per ricerche e/o consultazioni di siti il cui contenuto informativo appaia osceno, offensivo alla morale nonché alla pubblica decenza, a contenuto discriminatorio di taluni o razzista, a sfondo politico e/o religioso;
• per trasferire sulla postazione dell'utente programmi e/o file di dati relativi a progetti od obiettivi estranei all'utente o per finalità personali (come ad esempio file il cui contenuto sia protetto da diritto d'autore);
• per ricerche e/o consultazioni, all'interno dell'orario di lavoro, in maniera ripetuta e unicamente per scopi personali, di siti il cui contenuto informativo non sia attinente con l'attività lavorativa dell'utilizzatore;
• per ricerche e/o consultazioni palesemente incompatibili con i fini istituzionali dell'Azienda. È comunque vietato l'uso dello strumento nei casi configurati dalla normativa vigente come reato, in particolare:
diffusione di virus, "cavalli di troia" o altri programmi la cui azione consista nel sabotaggio, distruzione, alterazione o visione del contenuto informativo delle postazioni degli altri utenti, degli elaboratori aziendali e dei dati in essi contenuti, anche qualora l'obiettivo sia all'esterno della rete aziendale;
• per attività di furto di dati aziendali o di altri utenti, organismi e/o aziende;
• per attività di hackeraggio e pirateria informatica in generale.
I servizi aziendali potranno richiedere l'accesso a particolari siti istituzionali in "modalità privilegiata", ovvero senza disporre delle credenziali per la generica navigazione Internet oppure con una disponibilità di banda superiore al normale.
Lo S.T.I. provvederà ad evadere queste richieste compatibilmente con le risorse tecniche a disposizione.

Art. 6 - Rilevazione statistica delle attività

Accesso ad Internet

Le operazioni di accesso ad Internet potranno essere memorizzate per finalità di sicurezza del sistema con la gradualità prevista dalla normativa vigente.
La rilevazione statistica delle attività avviene attraverso i file di "log" generati dai sistemi.
I log non sono accessibili per la consultazione e la loro tenuta avviene a cura degli Amministratori di Sistema nominati secondo le modalità previste dalla normativa vigente e dai regolamenti aziendali in merito. Questi log non sono oggetto di operazioni di backup.
Nell'ambito dell'attività autorizzata alla navigazione in Internet, lo S.T.I. provvede ad effettuare elaborazioni statistiche utilizzando i dati di "log" dell'uso del servizio, che contengono:
• data e ora dell'accesso;
• nome del sito richiamato per la consultazione;
• esito della consultazione;
• tipologia di operazione richiesta e informazioni sugli eventuali file scaricati;
• numero di byte trasferiti dall'elaboratore remoto e viceversa. Qualora lo S.T.I. riscontri le seguenti anomalie:
• traffico superiore del 20% rispetto alla media dell'ultimo semestre;
• utilizzo di porte e/o protocolli non utilizzati dai programmi aziendali;
• contemporanea presenza di sessioni parallele dirette al medesimo sito remoto;
• traffico dati diretto a siti presenti nella black-list;

agli utenti verrà inviato un avviso generalizzato che informa della sospensione, per un periodo limitato e definito nella stessa informativa, dei controlli anonimi e del fatto che i log di sistema verranno utilizzati per l'individuazione di tali anomalie. Durante questo periodo, in aggiunta alle informazioni enunciate in precedenza, verrà rilevato anche l'indirizzo IP di partenza della navigazione. Al termine del periodo di osservazione questi log saranno distrutti a cura dello S.T.I..
In ogni caso non verranno estratte statistiche a livello individuale, bensì su base aggregata per area, settore o ufficio. In nessun caso i log del sistema generati sono usati come strumento di controllo dell'operato dell'utente. Da essi non è ricavabile alcuna informazione relativa al tempo trascorso nelle varie navigazioni dai singoli utenti.
L'Azienda utilizzerà le risultanze dell'elaborazione statistica dei log per aggiornare una black-list finalizzata ad impedire la navigazione verso siti vietati o non attinenti agli scopi istituzionali dell'Azienda.
Qualora un sito bloccato venga segnalato, attraverso l'apposita pagina di richiesta di sblocco, di interesse aziendale e riconosciuto come tale dallo S.T.I., lo stesso sarà rimosso dalla black-list e la rimozione avrà efficacia nei confronti di tutti gli utenti.
I log potranno essere oggetto di provvedimenti dell'Autorità Giudiziaria e Amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo. A seguito di specifica richiesta da parte delle Autorità preposte essi verranno memorizzati in forma non anonima, conservati e consegnati secondo le istruzioni ricevute da parte delle Autorità stesse.

Posta elettronica

Non viene tenuto alcun log relativo all'attività svolta dagli utenti con il servizio di posta elettronica.
L'unico log generato dal sistema è di tipo diagnostico con la finalità di individuare eventuali problemi in invio e ricezione della posta e la sua conservazione è limitata nel tempo a 30 giorni solari da un sistema automatico di cancellazione. Questo log non è oggetto di operazioni di backup.
I messaggi inviati e ricevuti in modalità web vengono conservati sul server di posta fino alla loro cancellazione da parte dell'utente. I messaggi inviati e ricevuti mediante software client installato su PC restano memorizzati esclusivamente sul PC dell'utente.
L'Azienda sta valutando l'introduzione di un sistema di gestione della posta elettronica aziendale che consenta l'archiviazione dei messaggi e-mail inviati e ricevuti a scopo di ripristino degli stessi a seguito di distruzione, danneggiamento, perdita sia volontaria che accidentale, ritenendo la posta elettronica una banca dati di interesse strategico.

Accesso remoto alle postazioni

Gli strumenti di accesso remoto utilizzati dallo S.T.I. non costituiscono in alcun modo controllo a distanza dell'attività del lavoratore.
Ogni accesso remoto da parte di personale tecnico autorizzato ad una stazione di lavoro avviene solo per finalità di assistenza tecnica al fine di aggiornare/ripristinare le condizioni di funzionamento ottimali e/o di installarne delle nuove.
Ogni accesso avviene dietro consenso dell'utente espresso mediante la pressione di un tasto (o mediante altre azioni che denotino volontarietà e consapevolezza degli utenti); ciò quindi implica la presenza dell'utente davanti al monitor che ha piena visione delle operazioni svolte dall'addetto all'assistenza remota e ha facoltà di interromperle in ogni istante.
L'accesso remoto alle postazioni è ammesso senza consenso dell'utente se esse si trovano in modalità disconnessa ("logout"), e in tal caso l'utente remoto accede al sistema con le proprie credenziali senza accedere ai contenuti dei profili personali degli utenti del PC.
Nel caso in cui, per problematiche tecniche urgenti ed improcrastinabili, si renda necessario accedere con le credenziali di uno specifico utente, e questi non sia disponibile, verrà resettata la sua password e lo stesso dovrà provvedere alla sostituzione della password al primo collegamento.
In questi particolarissimi casi lo S.T.I. documenterà dettagliatamente ogni operazione effettuata con le credenziali dell'utente, ed informerà lo stesso con la massima tempestività.
In nessun caso lo S.T.I. chiede la password di accesso degli utenti, che comunque non è conosciuta dal personale tecnico.

Art. 7 - Configurazioni hardware e software

Le postazioni di lavoro utente vengono predisposte e configurate per il corretto uso dei S.I.A. dallo

S.T.I..
L'utente si impegna a mantenere la corretta configurazione della postazione di lavoro che utilizza.
Le politiche relative ai software di gestione della sicurezza sono gestite centralmente e non è richiesta all'utilizzatore alcuna operazione manuale in merito.
A tal fine le postazioni di lavoro sono normalmente configurate per consentire l'accesso dell'utente solamente in modalità non privilegiata. Nel caso in cui a causa di particolari requisiti tecnici si renda necessario elevare i privilegi informatici dell'utente, quest'ultimo è maggiormente tenuto a preservare la configurazione della propria macchina così come impostata dallo S.T.I..
Qualora durante un intervento di manutenzione, i tecnici S.T.I. rilevino postazioni utente non conformi agli standard aziendali autorizzati, in mancanza di una specifica precedente deroga, gli stessi procederanno d'ufficio a ripristinare tali postazioni secondo gli standard definiti.
Nel caso in cui l'utente ritenga siano necessarie modifiche alla configurazione, ivi compresa l'installazione di nuovi programmi, dovrà formulare una richiesta allo S.T.I. che provvederà ad autorizzare o meno la richiesta, in quanto ogni modifica implica potenziali ricadute sulle corrette funzionalità delle procedure aziendali.
L'utente è responsabile delle attrezzature informatiche a lui assegnate, anche temporaneamente, e deve custodirle con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro, soprattutto nel caso di attrezzature portabili.
L'Azienda persegue una politica di centralizzazione nella gestione dei dati aziendali, per cui progressivamente le gestioni locali di dati scompariranno sostituite da gestioni centralizzate su server, qualora ciò sia tecnicamente possibile. Fino a che questo processo non sarà stato portato a compimento potranno esistere gestioni locali di dati su stazioni di lavoro personali (personal computer non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati) la cui tutela è demandata a all'utente finale.
L'effettuazione dei salvataggi con frequenza opportuna – almeno comunque settimanale – su supporti magnetici e la conservazione degli stessi in luogo idoneo - possibilmente sotto chiave e in contenitori ignifughi - è compito del singolo dipendente che usa la stazione (nel caso di stazioni di lavoro usate da un solo utilizzatore) o da un incaricato opportunamente individuato dal responsabile del trattamento nel caso di stazioni di lavoro condivise.
Ove è già presente un file server è fatto divieto di memorizzare in locale sulle stazioni di lavoro dati sensibili, che vanno salvati sui file servers. Nel caso in cui l'utente sotto la propria responsabilità

memorizzi anche solo per brevi periodi dati in locale sulla stazione di lavoro, dovrà gestire i requisiti minimi di sicurezza della stessa.
Tutti i pc devono avere il programma antivirus installato e configurato per l'aggiornamento automatico; nel caso in cui si verifichi la non rispondenza della stazione di lavoro a tale requisito si è pregati di rivolgersi allo S.T.I. Aziendale

Art. 8 - Utilizzo dei supporti di memorizzazione

È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili. Deroghe a tale regola sono possibili solo nei casi in cui sia possibile dimostrare il corretto uso dei supporti di memorizzazione ai sensi del D.L. 196/2003 Allegato B, punti 21 e 22:
• è possibile il reimpiego del supporto solo nel caso non siano più recuperabili le informazioni precedentemente memorizzate;
• nel caso non sia possibile garantire il requisito di cui al punto (1), il supporto removibile dopo l'uso andrà distrutto.
In generale i supporti di memorizzazione, anche non removibili, che contengono dati personali o sensibili, nel caso in cui non possano essere cancellati in maniera da renderne irrecuperabile il contenuto, una volta dismessi (per es. per obsolescenza o per guasto) dovranno essere distrutti o smaltiti in maniera tale che il contenuto non sia più recuperabile.

Art. 9 - Dismissione o cessione di supporti informatici

I supporti informatici non più necessari e contenenti dati devono essere resi inutilizzabili prima di dismetterli.
Questa operazione può essere effettuata distruggendo i supporti o sottoponendoli a cancellazioni logiche definitive con appositi software.
I supporti che dovessero essere ceduti a terzi vanno puliti sottoponendoli a cancellazioni logiche

definitive con appositi software.
Lo S.T.I. è a disposizione per ogni informazione di dettaglio al riguardo.

Art. 10 - Modalità di prestazione dei servizi

L'Azienda si impegna a fornire continuità ai servizi erogati, riservandosi la possibilità d'interromperli per le manutenzioni ordinarie o in caso di situazioni straordinarie (ad es. attacco informatico) che possano compromettere integrità, disponibilità e riservatezza dei dati aziendali. Qualora possibile le interruzioni saranno preventivamente comunicate agli utenti.
Per migliorare la qualità o la sicurezza dei servizi e dei sistemi informatici attualmente predisposti, l'Azienda valuterà con attenzione eventuali osservazioni, suggerimenti ed indicazioni che gli utenti faranno pervenire allo S.T.I..
L'operatività specifica del personale S.T.I., per la peculiare attività che svolge, in particolare per quanto riguarda la sperimentazione di nuove tecnologie da introdurre eventualmente in Azienda, è disciplinata in apposito documento di incarico.

Art. 11 - Backup e protezione dati sensibili

Lo S.T.I. provvede al salvataggio periodico delle banche dati prodotte dai Sistemi Informatici Centralizzati. La periodicità è indicata nel Documento Programmatico sulla Sicurezza (D.P.S.).
Gli utenti possono richiedere allo S.T.I. la creazione di cartelle condivise tra più utenti. Lo S.T.I., dopo una breve istruttoria, valuta se procedere e, in caso affermativo, provvede alla creazione sui propri server di tale cartella ed alle configurazioni sui PC degli utenti interessati. Tale cartella viene altresì inserita nei backup automatici.
Costituiscono dati di rilevanza aziendale soltanto quelli memorizzati sui server in proprietà gestiti dallo S.T.I.. Gli utenti non devono avere dati personali o sensibili memorizzati sui PC aziendali. Se

ciò avviene, l'Azienda non è responsabile di tali dati e non ne garantisce il periodico salvataggio né tantomeno il ripristino in caso di necessità.
Rimane comunque responsabilità dell'utente la cura e la protezione di eventuali file contenenti dati riservati e/o sensibili memorizzati sul proprio PC.

Art. 12 - Buon uso della rete e delle attrezzature aziendali di comunicazione

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive di azienda. In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione dello S.T.I.. È' altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro - o di altri dispositivi direttamente connessi alla rete, dati o fonia - per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni:
• divieto di condividere cartelle in rete (né dotate di password, né sprovviste di password) se non espressamente autorizzate dallo S.T.I. Aziendale;
• divieto di alterare la configurazione di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc…), comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in rete, browsing di risorse di rete, ecc…);
• è vietato intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia.
E' vietata l'installazione non autorizzata di modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'azienda.
E' vietata l'installazione non autorizzata di apparati di rete di qualsiasi tipo – hub, switch, router, access point WI-FI, access server, ecc… -.
E' vietata l'installazione di qualsiasi attrezzatura informatica o di comunicazione non espressamente autorizzata dallo S.T.I. Aziendale.
E' vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il by-pass delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino dai Firewall Aziendali o dagli altri accessi autorizzati e presidiati.
L'utente è inoltre tenuto a conservare con la massima cura eventuali dispositivi per l'accesso ai sistemi aziendali e ad usarli conformemente alle specifiche indicazioni d'uso. La perdita o

danneggiamento degli stessi sarà sanzionata.
I responsabili delle varie macro articolazioni organizzative, di concerto con i responsabili del trattamento e con il Servizio S.T.I., sono responsabili della adozione degli atti e delle misure organizzative necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'Azienda

Art. 13 - Virus e altro Malware

Si invitano gli utenti:
• alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione removibile sia stato utilizzato su un computer diverso dal proprio (supponendo che il proprio PC sia immune da infezioni) occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione, in quanto potenzialmente infetto;
• in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte;
• è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure. Nel caso pervenga un messaggio di tale natura

procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato, avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri. Nel caso si abbia notizia di un nuovo tipo di virus, comunicare tale informazione all'ufficio CARP del Servizio S.T.I. Aziendale (**cedarearetepc@aou.mo.it**) e non inviare indiscriminati messaggi a tutti i propri conoscenti: questo evita l'ingenerarsi di falsi allarmi e di inutili catene di Sant'Antonio.

Art. 14 - Internet

E' vietato l'utilizzo personale e non istituzionale della connessione a internet aziendale.
Tutti gli accessi ad Internet vengono registrati sul sistema di sicurezza aziendale in appositi file di log, come specificato all'Art. 6 del presente documento.
Tali log sono indispensabili all'Azienda per poter costantemente monitorare il corretto funzionamento del sistema nella sua globalità e per poter effettuare statistiche periodiche sull'uso del sistema, entrambi su base anonima. I log saranno trattati in maniera tale da fornire informazioni in maniera aggregata in modo da precludere l'immediata identificazione degli utenti, a meno che non vi siano specifiche ragioni per accedere al dettaglio massimo, cioè alle informazioni di tipo nominativo.
l'Azienda si riserva di filtrare l'accesso a siti che risultino non in relazione con le attività istituzionali; il filtraggio verrà attuato mediante l'inserimento del sito in una cosiddetta "Black list" ovvero nell'inserimento del sito in una categorizzazione, eventualmente predisposta anche da fornitori esterni specializzati; la lista dei siti inaccessibili o delle categorie potrà essere chiesta alla direzione del Servizio ICT Aziendale da chiunque e, in caso di motivate ragioni, potrà essere autorizzata la navigazione sul sito mediante rimozione dalla lista di esclusione; l'esclusione dei siti verrà operata periodicamente in base all'analisi di dati aggregati. A tal proposito, nel corso del 2015 è stata effettuata una modifica delle impostazioni del server proxy, al fine di limitare il numero dei siti a cui gli operatori possono accedere liberamente e prevenire così casi di navigazione indebita: rimane salva la possibilità di richiedere alla direzione del Servizio ICT Aziendale, di accedere ad uno o più siti bloccati, motivandone la necessità.
A titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:
• Servirsi o dar modo ad altri di servirsi della stazione di accesso a Internet per attività non istituzionali, attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
• Scaricare software dalla rete; eventuali necessità dovranno essere appositamente richieste allo S.T.I. che provvederà a eseguire fisicamente lo scarico da stazione protetta, applicare le misure antivirus relative e consegnare il software al richiedente;
• Utilizzare Internet Provider diversi da quello aziendale e la connessione di stazioni di lavoro aziendali alle reti di detti provider con sistemi di connessione diversi (es. modem o chiavette GSM) da quello centralizzato;

• Usare la rete in modo difforme da quanto previsto dal presente documento e dalle leggi penali, civili e amministrative in materia di disciplina dell'attività e dei servizi svolti sulla rete;
Non è consentito all'utente di produrre, pubblicare o manutenere siti web diversi da quello ufficiale aziendale mediante la rete aziendale e/o i S.I.A., salvo specifica autorizzazione scritta da parte della Direzione Aziendale o di Ufficio da questa espressamente delegato.
È altresì vietato utilizzare il sito aziendale, sia mediante la pubblicazione che l'inserimento di link a siti esterni, per pubblicizzare e/o promuovere attività non confacenti o addirittura in concorrenza con le attività erogate dall'Azienda Ospedaliero - Universitaria di Modena.
È diritto di ogni servizio chiedere di inserire uno spazio informativo (tecnicamente consistente in una o più "pagine", collegate tra loro ed alla "home page" aziendale) sul sito aziendale, di cui è direttamente responsabile anche per il contenuto e la correttezza delle informazioni.
A tale proposito i servizi dovranno fare richiesta all'Ufficio Comunicazione segnalando gli identificativi delle persone che potranno inserire informazioni sul sito e chi sarà il responsabile che ne autorizzerà la pubblicazione.

A tal fine lo S.T.I. provvederà a creare uno spazio web sul sito interno e/o sul sito pubblico, collegandolo alla pagina iniziale, o nella sottopagina eventualmente di riferimento.
Lo S.T.I. mette a disposizione il proprio supporto tecnico per la soluzione di eventuali problemi relativi all'applicazione delle procedure previste dal presente articolo, fatto salvo il fatto che l'inserimento e l'aggiornamento delle informazioni sono sempre a carico dei singoli servizi.
È' fatto divieto agli utenti di utilizzare il logo aziendale nei siti personali senza espressa autorizzazione del responsabile dell'Ufficio Comunicazione.
Si applicano in ogni caso le norme dei Codici deontologici professionali.
È' di norma vietato realizzare funzioni di hosting e/o housing, salvo specifica autorizzazione scritta da parte della Direzione Aziendale o di Ufficio da questa espressamente delegato.

Art. 15 - Servizio di Posta Elettronica

Il Servizio Informatico fornisce due distinte tipologie di account di e-mail:
• account di servizio, il cui nome richiama il servizio in cui lavora l'utente;
• account legati al nominativo dell'utente richiedente.
L'account di servizio deve comunque essere associato ad almeno un altro account nominativo di utente e non può essere utilizzato per l'invio di messaggi, ma solo in ricezione. Sarà compito dello S.T.I. fare in modo che i messaggi inviati a detto indirizzo siano smistati a tutti gli appartenenti al gruppo a cui è associato l'account di equipe.
Ogni account nominativo di posta ha uno spazio dedicato a disposizione di 1000MB. Il raggiungimento di tale limite implica l'impossibilità di utilizzare, in tutto o in parte, il servizio. Al raggiungimento del 80% dell'occupazione dello spazio disponibile viene segnalato all'utente mediante un messaggio di posta elettronica.
Gli utenti possono richiedere allo S.T.I. l'estensione dello spazio dedicato. Lo S.T.I., dopo una breve istruttoria, valuta se procedere e, in caso affermativo, provvede all'assegnazione di una diversa dimensione dello spazio dedicato alla posta.
Tutti i possessori di una casella di posta elettronica nominativa sono tenuti, quando possibile, a consultare quotidianamente la propria corrispondenza ed a provvedere tempestivamente allo scarico della stessa. Si ricorda che la consultazione via web non comporta lo scaricamento della posta dal server aziendale, operazione possibile soltanto con un client appositamente configurato sulla propria stazione di lavoro.
Per ottenere un account di posta elettronica è necessario seguire le indicazioni previste all'art. 4 del presente "Disciplinare".
È' possibile consultare la posta elettronica non ancora scaricata o inviare nuovi messaggi collegandosi direttamente al sito internet aziendale, per consentire agli utenti fuori sede di continuare ad utilizzare il servizio.
Per inviare e ricevere e-mail relative ad argomenti inerenti l'attività lavorativa è obbligatorio utilizzare l'account aziendale.
È' vietato l'utilizzo dell'account di posta elettronica aziendale per comunicazioni estranee all'attività lavorativa, per un uso personale e non istituzionale
E' vietato l'utilizzo della posta elettronica per l'invio di dati sensibili. In particolare è vietato un

uso di tale strumento dal quale possa derivare la possibilità, anche indiretta o preterintenzionale, di rilevare le opinioni politiche, religiose o sindacali dell'operatore, le sue inclinazioni sessuali, il suo stato di salute.
È' consentito un moderato utilizzo di provider esterni di posta elettronica per comunicazioni personali, esclusivamente in modalità web, con l'avvertenza che l'Azienda non può fornire supporto in caso di impossibilità di raggiungere i siti web di tali provider a causa delle particolari configurazioni della rete finalizzate a massimizzare la sicurezza. Inoltre la modalità di consultazione di tali informazioni deve essere compatibile con i vincoli di sicurezza del sistema aziendale e deve avvenire in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda
Tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail con virus, effettua i seguenti controlli:
• blocco delle e-mail con allegati potenzialmente pericolosi (file con estensioni EXE, .COM, VBS, .PIF, .SCR, .SYS, .BIN, .OVL, .DRV, .OVY, .LNK)
• blocco delle e-mail con dimensioni complessive (messaggio di posta + allegati) superiori a 7 Mb

• blocco delle e-mail con più di 30 allegati e/o più di 50 destinatari
• in particolari situazioni, ad esempio massicce ricezioni di e-mail infette, il Servizio S.T.I. Aziendale si riserva di bloccare e cancellare le e-mail che contengano particolari allegati o che abbiano nell'oggetto o nel corpo del messaggio particolari parole e/o frasi riconducili alla violazione di sicurezza o a codice pericoloso.
Al fine di garantire il corretto funzionamento della posta elettronica aziendale e di evitare la proliferazione del traffico indebito – che in termine tecnico viene chiamato SPAM – l'Azienda ha in uso un sistema AntiSPAM che filtra tutta la posta gestita. Il sistema AntiSPAM utilizza regole euristiche per decidere l'inoltro o meno di un messaggio. Le regole di filtraggio possono causare:
• il passaggio di SPAM qualora non sufficientemente selettive;
• il mancato inoltro di posta elettronica erroneamente giudicata dal sistema come SPAM.
Per le ragioni sopra indicate si vieta l'utilizzo della posta elettronica di materiali in copie uniche o comunque per l'invio di comunicazioni di cui debba essere garantito l'inoltro al destinatario.
Il sistema di posta elettronica in uso, e concesso in utilizzo, non è un sistema di posta certificata, non vi è pertanto la garanzia della consegna o della ricezione dei messaggi di posta, né fornisce garanzia di riservatezza relativamente ai messaggi inviati in quanto non usa alcuna tecnica di crittografia dei contenuti o di protezione delle autenticazioni. È pertanto fatto divieto di inviare materiali che non siano compatibili con tali caratteristiche del servizio.
L'Azienda mette a disposizione funzionalità di avviso in caso di assenza prolungata dell'operatore, che sfruttano le peculiarità del sistema di posta elettronica e possono fornire coordinate di altri riferimenti all'interno dell'Azienda tali da garantire il corretto funzionamento dei servizi.
L'attivazione di tali misure sarà a cura dell'operatore che dovrà avvisare le locali sedi del Servizio S.T.I. Aziendale di attuare la misura o attuarla in autonomia se tecnicamente non in grado; qualora l'operatore non abbia adottato tale misura e l'assenza si protragga per più di una settimana, il responsabile del trattamento potrà richiedere al Servizio S.T.I. Aziendale l'adozione di tale misura.
Ogni assegnatario di indirizzo di posta elettronica aziendale potrà, in caso di necessità, dirottare la propria posta elettronica su un diverso indirizzo di posta elettronica personale o di un fiduciario; nel caso non sia in grado di attuare detta misura in autonomia, potrà chiedere al Servizio S.T.I. Aziendale la messa in atto della misura; della attuazione di tale misura verrà tenuta traccia e verrà data notizia al lavoratore interessato alla prima occasione utile.
Qualora vengano inviati messaggi di posta elettronica che prevedano che l'eventuale risposta possa essere conosciuta da più persone nell'ambito dell'Azienda, occorrerà rendere edotto di ciò il destinatario.
Fatte salve le limitazioni di cui ai punti precedenti l'Azienda favorisce l'utilizzo della posta elettronica come strumento per la rapida comunicazione fra i dipendenti, fra dipendenti e cittadini, fra pubbliche amministrazioni, purché queste comunicazioni siano parte delle attività istituzionalmente previste e compatibili con le mansioni proprie di ogni operatore. Fatte salve le limitazioni precedentemente esposte, alla trasmissione telematica di atti e documenti all'interno dell'Azienda per posta elettronica è riconosciuta la stessa validità della trasmissione per via cartacea; in particolare potranno essere trasmessi atti deliberativi, disposizioni dirigenziali e documenti in genere che non contengano dati

sensibili e il cui mancato recapito non ingeneri danni per l'azienda, per i dipendenti o per altri.
L'utilizzo della posta elettronica, in questi casi, potrà sostituire completamente l'invio di carta. Atti o documenti aventi valenza generale possono essere comunicati a tutti o a grande parte dei dipendenti dell'Azienda; ciò può avvenire tramite l'utilizzo di apposite liste di distribuzione che sono messe a disposizione in posta elettronica; esigenze particolari od occasionali di comunicazione ad un numero di utenti il cui volume o la cui qualità non sia già stata prevista dovranno essere inoltrate dal Servizio S.T.I. Aziendale.

Art. 16 - Comunicazioni di massa

È' fatto obbligo agli utenti segnalare allo S.T.I. l'eventuale ricevimento di messaggi, sia da utenti interni che esterni, appartenenti ad una delle seguenti categorie:
• "mail spamming" e "catene di S. Antonio";

• aventi contenuto diffamatorio per l'Azienda od i suoi dipendenti;
• aventi contenuto moralmente deplorevole, scandaloso, propagandistico per correnti politiche o fazioni religiose;
• aventi contenuto non attinente l'attività lavorativa ed il cui ricevimento sia "non gradito" all'utente;
• aventi il fine di "intasare" le caselle di posta elettronica.
La segnalazione va indirizzata esclusivamente via e-mail all'indirizzo **cedarearetepc@aou.mo.it**, inoltrando la e-mail sospetta.
Gli utenti interni che attuano uno dei comportamenti vietati verranno segnalati al Dipartimento Risorse Umane per le eventuali sanzioni disciplinari.
Per quanto riguarda comunicazioni da inviare in maniera massiva a tutte le caselle di posta aziendali, in genere per comunicazioni che rivestono particolare importanza per un congruo numero di utenti, l'autorizzazione deve essere ottenuta dall'Ufficio Comunicazione, che valuterà e approverà il testo proposto per l'invio.

Art. 17 - Data breach

Dal mese di agosto 2015, in ottemperanza ad un obbligo sancito dal Garante Privacy è stata introdotta e diffusa tra tutti i dipendenti una procedura per la comunicazione obbligatoria e tempestiva al Garante (entro le 48 ore dalla conoscenza del fatto) di eventuali violazioni dei dati o incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle banche dati dell'Azienda – c.d. data breach[1].
Pertanto chiunque in Azienda sospetti sia avvenuto un data breach deve immediatamente comunicarlo allo S.T.I., utilizzando l'indirizzo email: **security@aou.mo.it**.

Art. 18 - Cessazione della disponibilità dei servizi informatici aziendali

Ai sensi del presente "Disciplinare", la disponibilità dei servizi informatici aziendali cesserà per l'utente nei seguenti casi:
1) qualora non sussistesse più la condizione di dipendente o di collaboratore esterno. Questo evento dovrà essere comunicato tempestivamente da parte del responsabile del servizio cessante allo S.T.I., in modo da poter eliminare dai S.I.A. tutte le abilitazioni;
2) qualora non fosse confermata o venisse revocata l'autorizzazione all'uso fornita dal Responsabile; il quale dovrà comunicare l'evento come al punto precedente;
3) qualora avvenisse il trasferimento di un utente da un servizio ad un altro. Il Responsabile del servizio cessante dovrà comunicare tempestivamente la cessazione del rapporto, mentre il Responsabile del servizio subentrante dovrà autorizzare le nuove abilitazioni con le procedure descritte all'art. 4 del presente "Disciplinare";

Art. 19 - Altri strumenti di comunicazione aziendale: Telefoni fissi, telefoni mobili, ecc…

E' vietato l'utilizzo personale e non istituzionale del telefono.
L'azienda, mediante configurazioni sugli apparati tecnologici, impedisce l'effettuazione di chiamate dalla rete aziendale verso determinate categorie di numeri: ad esempio numeri a pagamento per servizi particolari che si giudicano non interessanti dal punto di vista istituzionale, ecc….
Ogni operatore che abbia la necessità di utilizzare, per fini istituzionali, una classe di numeri non abilitata potrà richiedere una specifica abilitazione.

1 Fra gli eventi che possono essere ascritti ad un data breach, pur essendo l'elenco non esaustivo, vi sono:l'accesso abusivo

a dati personali, sensibili o giudiziari contenuti nelle banche dati aziendali; la copia abusiva per immagine su supporto informatico di documenti analogici contenenti dati personali, sensibili o giudiziari; la perdita o il furto di attrezzature aziendali – PC portatili, PC fissi, dispositivi di memorizzazione, ecc… che contengano dati personali, sensibili o giudiziari; attacchi condotti da persone o software – malware - che ottengano l'accesso alle banche dati aziendali o più in generale eventi che possano portare ad accessi indebiti o alla cattura di dati di accesso e di identificazione - user name e password.

pag. 14

Per fini di controllo della spesa telefonica l'Azienda tiene traccia delle telefonate effettuate, qualora queste inducano un onere economico per l'Azienda; non sono ad esempio tracciate le telefonate in ingresso che sono tipicamente non onerose in termini economici. Viene registrato:

• il numero del chiamante;
• il numero chiamato;
• la data e ora di inizio della telefonata e la data e ora di fine della stessa

Tutti i log sopra citati vengono conservati dall'Azienda un anno solare in maniera disaggregata per poter confrontare gli andamenti di costo con i dati aggregati degli anni precedenti. I dati disaggregati dal primo gennaio dell'anno al trentuno dicembre dell'anno potranno essere tenuti fino alla fine di marzo dell'anno successivo per i controlli istituzionali, dopo di che dovranno essere aggregati in maniera tale che possano essere utilizzati per i confronti con i periodi successivi. I controlli verranno effettuati in maniera non nominativa e aggregata – ad esempio aggregando i dati per edificio o per unità erogante; qualora i dati evidenzino anomalie tali da giustificare controlli aggiuntivi, potranno essere ulteriormente approfonditi. Normalmente sarà necessario adottare una gradualità nei controlli che preveda prima il controllo del dato aggregato e la notifica di eventuali anomalie e solo successivamente, qualora il problema persista, un controllo sui dati disaggregati.

Qualora l'integrità del sistema tecnologico dell'azienda o la gravità del fatto lo rendano necessario sarà possibile accedere immediatamente al dato disaggregato; qualora possibile, gli approfondimenti sui dati che si rendessero necessari saranno condotti con verifiche a campione.

In generale tutte le verifiche dovranno rispettare i criteri della pertinenza e non eccedenza rispetto al fine di controllo amministrativo proprio dell'Azienda; qualora le verifiche portino all'accertamento della violazione delle presenti regole o più in generale all'accertamento di utilizzi impropri, l'Azienda si riserva di adottare le opportune misure disciplinari e amministrative.

Art. 20 - Tutela del diritto d'autore

Vista la legge 248 del 18/08/2000 relativa alla tutela del diritto d'autore:

• E' vietata la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi, si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi;
• è fatto divieto ad ogni utilizzatore del sistema informativo aziendale scaricare, gestire in qualsiasi modo e trattare dati o informazioni che violino la normativa sulla tutela del diritto d'autore;
• qualora l'operatore nonostante tale divieto infranga tale normativa sarà penalmente e civilmente responsabile del proprio operato sollevando l'azienda da ogni responsabilità.

Art. 21 - Ulteriori istruzioni per la tutela delle informazioni gestite dagli operatori

Documentazione cartacea

• L'operatore, per tutto il periodo in cui effettua le operazioni di trattamento dei dati, non deve mai perdere di vista i documenti, adempiendo ad un preciso obbligo di custodia dei medesimi.
• L'operatore deve controllare che i documenti siano sempre completi ed integri.
• In caso di abbandono, anche temporaneo, dell'ufficio, l'operatore non deve mai lasciare incustoditi i documenti (sulla scrivania o su tavolini di reparto); è infatti necessario identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.); ove si utilizzi un contenitore/locale chiuso a chiave occorre accertarsi che non esistano duplicati abusivi delle chiavi e che le stesse siano in possesso solo di operatori autorizzati.
• Occorre in particolare accertarsi che nessun visitatore o terzo estraneo possa venire a conoscenza (anche per cause accidentali) del contenuto dei documenti.
• Al momento della consegna di documenti contenenti dati personali o sensibili ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate.

• La distruzione dei documenti contenenti dati personali o sensibili deve avvenire con modalità che rendano impossibile l'individuazione dell'interessato da parte di terzi non autorizzati (mediante apposita macchinetta tritatutto o distruzione manuale in piccoli pezzi).

Comunicazioni telefoniche e via fax

• Nel caso in cui sia necessario effettuare comunicazioni telefoniche agli interessati, occorre aver chiesto preliminarmente all'interessato medesimo l'autorizzazione a conferire con chi risponda all'apparecchio. In caso di risposta negativa l'operatore deve chiedere in alternativa un numero riservato.

• Occorre fare attenzione a discutere, comunicare o comunque trattare dati personali/sensibili per telefono in presenza di terzi non autorizzati che potrebbero inavvertitamente venire a conoscenza di tali dati.

• In caso di invio di documentazione a mezzo fax, bisogna prestare attenzione alla corretta digitazione del numero cui inviare il documento e verificarne l'esattezza; qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è opportuno anticipare l'invio del fax avvertendo il destinatario, assicurarsi che il ricevimento avvenga nelle mani del medesimo ed evitare che soggetti estranei o non autorizzati possano conoscere il contenuto della documentazione inviata.

• L'apparecchio fax deve essere sempre collocato in luogo non accessibile a terzi non autorizzati.

Utilizzo della fotocopiatrice e della stampante

• In caso di stampa o duplicazione non riuscite di documentazione contenente dati personali/sensibili, occorre evitare di gettare i fogli nel cestino senza aver provveduto a rendere illeggibile il contenuto dei dati.

• Qualora si utilizzi carta riciclata per fotocopie e stampe, occorre sempre accertarsi che non siano accidentalmente riportati dati personali e/o sensibili.

• Occorre utilizzare con attenzione le macchine fotocopiatrici di ultima generazione che possono scannerizzare e memorizzare il documento, talvolta conservando il file elettronico dello stesso.

Rapporti di front office

• **Rispetto della distanza di cortesia**: l'operatore di sportello deve prestare attenzione al rispetto dello spazio di cortesia e, se del caso, invitare gli utenti a sostare dietro le apposite linee/barriere delimitanti lo spazio di riservatezza.

• **Controllo dell'identità del richiedente**: nel caso di richieste di comunicazioni di dati (presentate per telefono o via fax) occorre verificare l'identità del soggetto richiedente (ad esempio formulando una serie di quesiti al fine di un accertamento sommario) e la sua legittimazione a ricevere le informazioni su quanto richiesto.

• **Identificazione dell'interessato e controllo dell'esattezza dei dati**: nel momento della raccolta di dati anagrafici (in particolar modo nel caso di cittadini stranieri) occorre fare attenzione alla digitazione ed all'inserimento corretto dei dati identificativi dell'interessato.

• **E' vietata la chiamata nominativa dell'utente**: nelle sale e negli spazi di attesa i nomi dei pazienti non devono essere divulgati ad alta voce; occorre utilizzare un sistema che prescinda dai dati anagrafici (es. codice alfanumerico, orario della prenotazione, ecc.). Eventuali deroghe ed eccezioni devono essere discusse con l'Ufficio Privacy.

Corretta comunicazione dei dati

• La richiesta di comunicazione o documentazione di dati personali e sensibili può essere evasa nei confronti dell'interessato o di un terzo a ciò delegato (per iscritto) o legittimato per legge (in casi dubbi rivolgere sempre richiesta di chiarimenti al responsabile del trattamento). In tal senso assoluta attenzione deve essere in particolare prestata nelle operazioni di consegna di referti diagnostici, cartelle cliniche, risultati di analisi e certificati.

• Devono comunque essere rispettate le modalità del controllo dell'identità del richiedente (vd. paragrafo "rapporti di front office").

• La comunicazione di dati idonei a rivelare lo stato di salute deve essere sempre effettuata da un medico o da personale sanitario a ciò delegato (art. 84 D.Lgs. 196/03).

• L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi nonché essere contenuto in busta sigillata,

evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

Rispetto della privacy in corsia

• Devono essere adottate soluzioni tali da prevenire, durante i colloqui, l'indebita conoscenza, da parte di terzi, di informazioni idonee a rivelare lo stato di salute (ad es. utilizzo, laddove possibile, di spazi riservati).
• Devono altresì essere adottate soluzioni tali da garantire il rispetto della dignità dell'interessato, in occasione di prestazione mediche particolarmente delicate (ad es. utilizzo di paraventi).
• L'interessato ricoverato, se cosciente e capace, deve essere preventivamente informato e poter decidere a chi possa essere data comunicazione della propria presenza in ospedale. Qualora l'interessato non possa essere interpellato in proposito, potranno essere fornite informazioni, anche telefoniche, sul passaggio o sulla presenza dello stesso al Pronto Soccorso o in altri reparti solo ai terzi legittimati come familiari e congiunti, previo accertamento sommario dell'identità del richiedente (es. mamma che contatti il Pronto Soccorso per avere notizie circa l'eventuale presenza del figlio nella struttura).
• Occorre porre in essere procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparto o strutture indicativa dell'esistenza di un particolare stato di salute (sono vietate ad es. le carrozzine che riportano per esteso il nome dell'unità operativa di appartenenza).
• E' vietata, in locali aperti al pubblico o di passaggio, l'affissione di liste di pazienti in attesa di intervento; in tali luoghi è vietata altresì l'affissione della turnistica degli operatori riportante la causa di assenza (es. malattia).
• Non devono essere visibili ad estranei documenti sulle condizioni cliniche del malato (es. cartelle cliniche/infermieristiche poste vicino al letto di degenza). Qualora fosse necessario mantenere la grafica ai piedi del letto, essa dovrà essere girata o comunque posizionata in modo tale da non poter essere immediatamente visibile da terzi estranei.

Art. 22 - Servizio deputato ai controlli

L'Azienda delega al Servizio Tecnologie dell'Informazione i controlli tecnici sui sistemi informatici previsti dalla presente linea guida e alle macro articolazioni gestionali la responsabilità complessiva del controllo del personale afferente alle unità organizzative di competenza.

Art. 23 - Comportamenti che danno luogo a segnalazione

Ai sensi del presente "Disciplinare", potranno essere segnalati al Dipartimento Risorse Umane, che valuterà le eventuali sanzioni disciplinari, gli assegnatari dei S.I.A. che porranno in essere uno o più dei seguenti comportamenti in aggiunta a quelli già indicati nell'art. 13:
a) installazione non autorizzata di hardware o software;
b) alterazione non autorizzata della configurazione hardware o software della stazione di lavoro;
c) comunicazione o diffusione di credenziali di accesso a sistemi e procedure informatiche, nonché altre informazioni tecniche riservate;
d) scarico non autorizzato di materiale informatico estraneo all'attività lavorativa;
e) violazione in genere di norme del Codice Penale, nella parte in cui tratta dei reati informatici;
f) violazione di quant'altro stabilito nel presente "Disciplinare".

Art. 24 - Informativa

Il Titolare del trattamento dei dati è l'Azienda Ospedaliero - Universitaria di Modena.
I Responsabili del trattamento dei dati personali, a mezzo di strumenti informatici dell'Azienda, sono:

• Lo S.T.I. (nella persona del Direttore del Servizio) per quanto attiene alla gestione dei dati effettuata mediante i sistemi informativi aziendali, circa le modalità tecnologiche e gli strumenti utilizzati per l'erogazione del servizio, ivi compreso il profilo della sicurezza;
• I Responsabili del trattamento dei dati designati dal Titolare del trattamento con apposito provvedimento, per quanto attiene alle decisioni riguardo alla finalità ed alle modalità organizzative di utilizzo dei sistemi o servizi di competenza;
• i terzi che, in relazione ai servizi chiamati ad espletare per conto dell'Azienda, siano dalla stessa autorizzati all'utilizzo di sistemi informatici aziendali.

I diritti previsti dall'art. 7 del D.Lgs. 196/03 e in particolare il diritto di conoscere i dati che riguardano l'utente, il diritto di aggiornarli e il diritto di cancellare i dati eventualmente trattati in violazione di legge potranno essere esercitati rivolgendosi ai Responsabili del trattamento dei dati designati dal Titolare del trattamento con apposito provvedimento.
Il presente "Disciplinare" inizierà ad essere applicato dalla data dall'adozione del relativo provvedimento di approvazione e potrà essere soggetto in qualsiasi momento a modifiche ed aggiornamenti, dovuti ad innovazione tecnologica e/o a modifiche organizzative aziendali, nonché per il mutato quadro normativo di riferimento.
Tali variazioni saranno rese note a tutti i dipendenti tramite l'emanazione di nuovi provvedimenti deliberativi.