SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Regione Emilia Romagna

AZIENDA UNITA' SANITARIA LOCALE DI PARMA
Strada del Quartiere n. 2/a − Parma

* * * * *

VERBALE DELLE DELIBERAZIONI
DEL DIRETTORE GENERALE

Deliberazione assunta il 24/04/2013 N.254

Proposta n. 16915
Ufficio/Servizio proponente: DIREZIONE AMMINISTRATIVA

OGGETTO

AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DI CUI ALL'ALLEGATO B DEL D.L.VO 30/06/03 N. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI": ANNO 2013.

Il giorno 24/04/2013 alle ore 12:00 nella sede dell'Azienda Unità Sanitaria Locale di Parma − Strada del Quartiere n.2/a − Parma, il Direttore Generale, sentiti il Direttore Amministrativo e il Direttore Sanitario , ha adottato l'atto in oggetto specificato.

OGGETTO: AGGIORNAMENTO DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DI CUI ALL'ALLEGATO B DEL D.L.VO 30/06/03 N. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI": ANNO 2013.

IL DIRETTORE GENERALE

DATO ATTO che, con deliberazione n.° 166 del 31 marzo 2006 è stato approvato il documento programmatico sulla sicurezza, redatto ai sensi degli artt. 33 e seguenti e dell'allegato B del D.Lgs 30.06.2003 n. 196 "Codice in materia di protezione dei dati personali";

RILEVATO che il punto 19 dell'allegato B sopra citato prevede che entro il 31 marzo di ogni anno, il titolare del trattamento di dati sensibili e/o giudiziari rediga un documento programmatico sulla sicurezza contenente idonee informazioni riguardo a:

a) l'elenco dei trattamenti;
b) la distribuzione dei compiti e delle responsabilità;
c) l'analisi dei rischi a cui possono essere soggetti i dati trattati;
d) le misure da adottare per garantire l'integrità e la protezione;
e) i criteri e le modalità di ripristino dei dati in corso di danneggiamento e distribuzione;
f) la formazione per gli incaricati dei trattamenti;
g) i criteri per le misure di sicurezza per i dati il cui trattamento è affidato a soggetti esterni alla struttura del titolare;
h) i criteri adottati per la cifratura e/o la separazione di dati personali dai dati idonei a rivelare lo stato di salute e la vita sessuale;

PRESO ATTO che il D.L. n° 5 del 2012, convertito nella legge 4 aprile 2012 n° 35, all'art. 45 dispone la soppressione della lettera g) dell'art. 34, comma 1 del Codice della privacy ossia, per il trattamento dei dati con strumenti elettronici, non è più necessaria la tenuta di un aggiornato documento programmatico sulla sicurezza;

RILEVATO pero' che la succitata norma (non obbligatorietà dell'adozione del Documento Programmatico sulla Sicurezza) non abroga l'adozione delle misure di sicurezza per cui il Titolare del trattamento deve ridurre i rischi che incombono sui dati; il Titolare mantiene in capo a sé gli obblighi relativi alle misure di sicurezza di cui agli artt. 33 e seguenti ed all'allegato B; non sono state abrogate le sanzioni amministrative e penali nonché l'obbligo del Titolare di dimostrare di aver fatto tutto il necessario per evitare che il danno accadesse;

VISTA la deliberazione n° 221 del 16.04.2012 con la quale è stato approvato l'aggiornamento per l'anno 2012 del Documento programmatico per la sicurezza di cui all'allegato B del D.Lgs 30.06.2003 n° 196 "Codice in materia di protezione dei dati personali";

RITENUTO pertanto, alla luce di quanto sopra esposto, continuare ad approvare l'aggiornamento DPS in modo da dare evidenza alle attività svolte ed alla diligenza posta nella predisposizione delle misure minime di sicurezza e quindi di tutti gli atti possibili ad evitare danni derivanti dal trattamento dei dati personali;

ATTESO che gli articoli da 33 a 35 del D.Lgs 30.06.2003 n° 196 "Codice in materia di protezione dei dati personali" disciplinano l'adozione delle misure minime per il trattamento dei dati sia con l'ausilio che senza l'ausilio di strumenti elettronici;

DATO ATTO che nella direttiva del 27 novembre 2008, il Garante ha rimarcato la criticità del ruolo degli amministratori di sistema ed ha diramato indicazioni affinché i titolari dei dati personali adottino cautele volte a prevenire ed accertare eventuali accessi ai dati personali non consentiti, in particolare quelli realizzati con abuso della qualità di amministratore di sistema. In particolare ha disposto che:

1) le funzioni di amministratore di sistema debbano essere affidate con riferimento all'esperienza, alla capacità ed affidabilità del soggetto designato che deve fornire idonea garanzia del rispetto delle norme vigenti;
2) la designazione deve essere individuale e riportare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo autorizzato;
3) gli identificativi degli amministratori di sistema, con le funzioni ad essi attribuite, devono essere riportati nel DPS (Documento Programmatico sulla Sicurezza). Quando l'attività riguarda sistemi che trattano o permettono il trattamento di informazioni di carattere personale dei lavoratori, i Titolari, quali datori di lavoro, devono rendere conoscibile l'identità degli amministratori di sistemi utilizzando i sistemi idonei in atto in Azienda (informativa resa ai sensi dell'art. 13 del Codice oppure l'Intranet aziendale quale strumento di comunicazione). Se detti servizi sono affidati in outsourcing, il Titolare deve dì conservare specificatamente gli estremi identificativi delle persone fisiche preposte ad amministratore di sistema;
4) annualmente, l'operato degli amministratori di sistema deve essere verificato dal Titolare del trattamento al fine di controllare la rispondenza alle misure organizzative, tecniche e di sicurezza adottate relativamente al trattamento dei dati personali;
5) è stato adottato un sistema di registrazione degli accessi logici ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema. Dette registrazioni hanno la caratteristica di completezza, inalterabilità e possibilità di verifica della loro integrità. Queste registrazioni sono conservate per almeno sei mesi;

RICORDATO che con deliberazione n° 466 del 13 luglio 2009 è stata disposta la nomina ad "Amministratore di sistema" dell'Azienda USL di Parma dell'Ing. Andrea Toniutti, quale responsabile del Servizio Risorse Informatiche e Telematiche dell'Azienda e che allo stesso è stato dato l'incarico della conservazione degli estremi identificativi delle persone fisiche preposte all'attività di Amministratore di sistema per i Servizi dati in outsourcing;

RILEVATO che il Direttore del Servizio Risorse Informatiche e Telematiche congiuntamente al Direttore del Servizio Affari Generali, ha provveduto, sulla base delle rilevazioni effettuate presso le banche dati aziendali, i nuovi trattamenti e le ultime soluzioni informatiche, ad aggiornare il Documento Programmatico sulla Sicurezza - DPS -, nel testo allegato al presente atto, quale parte integrante e sostanziale;

PRESO ATTO che:
- con determinazione n° 90 del 2 marzo 2012 del Direttore del Servizio Risorse Umane e Sviluppo Organizzativo sono state accolte le dimissioni, a far data dal 1 marzo 2012, dell'Ing. Andrea Toniutti;
- con determinazione del Servizio Risorse Umane n.° 31 del 25.01.2012 è stata indetta una procedura selettiva per il conferimento dell'incarico del Direttore del Servizio RIT;
- con deliberazione n° 518 del 02.08.2012 sono stati approvati gli atti della procedura selettiva per il conferimento dell'incarico di Direttore del Servizio RIT ed è stato conferito detto incarico all'Ing. Debora Angeletti;
- che con determinazione n° 414 del 28.11.2012 del Direttore del Servizio Risorse Umane e Sviluppo Organizzativo è stato collocato a riposo per dimissioni volontarie il Dott. Erio Azzolini dal 01.03.2013;

- che a seguito della cessazione dal servizio del Dott. Erio Azzolini il Direttore Generale, con lettera prot. 19317 del 07.03.2013, ha attribuito la responsabilità del Servizio Affari Generali al Direttore Amministrativo dott.ssa Elena Saccenti;

DATO ATTO che il D.P.S**.** riporta, oltre all'analisi dei rischi, le misure di sicurezza già in atto e quelle da dover adottare, nonché la distribuzione dei compiti e delle responsabilità;

DATO ATTO altresì che nel D.P.S. vengono confermati i Responsabili dei trattamenti aziendali;

RITENUTO di nominare l'Ing. Debora Angeletti, responsabile del Servizio Risorse Informatiche e Telematiche, quale Responsabile della Sicurezza;

RITENUTO, inoltre, di confermare quale responsabile dei diritto di accesso dell'interessato ai propri dati personali nonché referente complessivo aziendale in materia di trattamento dei dati personali, il Direttore del Servizio Affari Generali, allo stato nella persona del Direttore Amministrativo Dott.ssa Elena Saccenti fino all'attribuzione dell'incarico di Direttore del Servizio stesso;

VALUTATO positivamente il documento elaborato che permette, oltre ad un adeguato e costante aggiornamento formativo del personale aziendale, di ottemperare alle disposizioni del Codice assicurando la protezione dei dati personali, sensibili e giudiziari trattati nell'ambito delle attività aziendali;

RITENUTO quindi di approvare l'aggiornamento del D.P.S. aziendale per l'anno 2013, nel testo allegato, avendo presente che lo stesso sarà costantemente adeguato, nel rispetto delle scadenze previste dal Codice, sia in ordine all'eventuale evoluzione della normativa, che per le innovazioni tecnologiche nonché specifiche azioni volte ad acquisire un maggior livello di sicurezza nella gestione dei dati;

SU PROPOSTA del Direttore Amministrativo;

ACQUISITO il parere favorevole del Direttore Sanitario;

DELIBERA

1) di approvare, nonostante la non obbligatorietà, l'aggiornamento del Documento Programmatico sulla Sicurezza per l'anno 2013 nel testo allegato, quale parte integrante e sostanziale, alla presente deliberazione;

2) di approvare le azioni di seguito indicate al fine di accrescere il livello di sicurezza nella gestione dei dati;

    a) avviare la realizzazione della nuova sala server dell'AUSL di Parma e del sito di Disaster Recovery secondo i dettami della DigitPA per garantire maggiore integrità, sicurezza e continuità dei servizi e delle strutture;
    b) introdurre strumenti informatici per la formalizzazione delle richieste di creazione nuove utenze, abilitazione ad applicativi aziendali in relazione alle mansioni e modifica delle stesse per cambiamento della collocazione aziendale;

c) procedere alla formalizzazione e raccolta dei documenti relativi all'incarico di Responsabili al trattamento esterno dei dati per tutti i fornitori esterni;
d) completare la messa in dominio delle postazioni client e l'integrazione di tutti gli applicativi con il sistema LDAP aziendale e la distribuzione alle farmacie e ai centri esterni di un certificato di accesso alla rete aziendale;
e) revisionare il contenuto dei seguenti allegati del DPS: T0301 Linee trasmissione dati, T0302 Elenco strutture aziendali, P0101 Elenco responsabili dei trattamenti, P0102 Elenco responsabili Esterni, T0304 Elenco server aziendali, T0305 Elenco connessioni VPN, P0104 Videosorveglianza, aggiornare quando se necessario il documento P0103 Regolamento AVEN;
f) procedere a una maggiore diffusione all'interno dell'Azienda di software per redazione di testi e fogli elettronici aderenti alle normative Dgit PA, ovvero di formati open, secondo le modalità indicate al cap 3.4 del documento allegato P0703;

3) di confermare i Responsabili dei trattamenti aziendali nelle figure individuate con la deliberazione n° 166 del 31 marzo 2006, quale adempimento al disposto di cui ai commi 2,3, e 4 dell'art. 29 del D.Lgs 30.06.2003 n° 196;

4) di nominare, quale Responsabile della Sicurezza l'Ing. Debora Angeletti, Dirigente Responsabile del Servizio Risorse Informatiche e Telematiche dell'Azienda;

5) di confermare quale Responsabile dei diritto di accesso dell'interessato ai propri dati personali nonché referente complessivo aziendale in materia di trattamento dei dati personali, il Direttore del Servizio Affari Generali, allo stato nella persona del Direttore Amministrativo Dott.ssa Elena Saccenti fino all'attribuzione dell'incarico di Direttore del Servizio stesso.

ALLEGATO ALLA DELIBERAZIONE N° 254 DEL 24/04/2013

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ANNO 2013

– Quadro normativo

Con decreto legislativo 30 giugno 2003, n.196 è stato emanato il "Codice in materia di protezione dei dati personali" (di seguito indicato come Codice) che riforma interamente la materia, abroga e sostituisce undici tra leggi e decreti, e introduce le nuove misure di sicurezza dei dati e dei sistemi. Tali disposizioni sono entrate in vigore dal 1`gennaio 2004, presentando alcuni cambiamenti in singole disposizioni anche a fini di semplificare alcuni adempimenti, ma secondo un'impostazione che prosegue nelle linee già tracciate nella precedente disciplina.
Il Codice, entrato in vigore il 1° gennaio 2004, ha confermato ed aggiornato la disciplina in materia di sicurezza dei dati personali e dei sistemi informatici e telematici introdotta nel 1996 (L.675/96).
Le misure di sicurezza nel loro insieme devono garantire la protezione dei dati personali e dei sistemi. Quindi i programmi informatici, gli strumenti elettronici utilizzati, il sistema informativo nel suo complesso, gli atti e i documenti cartacei, gli ambienti nei quali vengono svolte le operazioni di trattamento e gli archivi devono essere adeguatamente tutelati.

Le prescrizioni sulla sicurezza sviluppano sia i concetti di *integrità, confidenzialità* e *disponibilità* dei dati contenuti nei principali standard di sicurezza condivisi dagli esperti del settore, sia alcuni principi e raccomandazioni della direttiva 2002/58/CE del Parlamento Europeo e del Consiglio del 12 luglio 2002 relativi alla tutela della vita privata nel settore delle comunicazioni elettroniche.

In particolare le misure minime di sicurezza devono essere raccolte, gestite e controllate attraverso un *Documento Programmatico sulla Sicurezza così* come definito dal combinato disposto dell'art. 34 con le regole 19 e 26 dell'Allegato B al Codice "Disciplinare tecnico di misure minime di sicurezza". In particolare la regola 19 recita:

“Documento Programmatico sulla Sicurezza”

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1 l'elenco dei trattamenti di dati personali;

19.2 la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3 1'analisi dei rischi che incombono sui dati;

19.4 le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

19.5 la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6 la previsione di interventi formativi degli incaricati del trattamento, per renderli

edotti 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. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7 la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare;

19.8 per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato."

Nel Codice sono inoltre riportare le seguenti definizioni:

"trattamento": qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, 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 di dati, anche se non registrati in una banca di dati;

"dato personale": 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.*

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

"dati sensibili": i dati personali idonei a rivelare l'origine razziale ed etnica, le con*vinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;*

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

Distribuzione di compiti e delle responsabilità

– Le previsioni del Codice

Nel Codice sono individuate all'art. 4 le seguenti figure:

1) *titolare*: La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. In particolare: esercita il potere decisionale in ordine alle finalità ed alle modalità del trattamento, compreso il profilo della sicurezza.Formalizza per iscritto i compiti affidati ai responsabili di trattamento; impartisce loro le istruzioni e ne verifica periodicamente l'osservanza. Sottoscrive le comunicazioni al Garante per la protezione dei dati personali.

2) *responsabile*: La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.In particolare:deve garantire il pieno rispetto delle vigenti disposizioni di legge in materia di trattamento e delle istruzioni impartite dal titolare, anche per quanto riguarda il profilo della sicurezza, verificandone il recepimento e l'attuazione entro la propria area di competenza.

3) *incaricati*: Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.In particolare l'incaricato deve: elaborare i dati per cui è stato autorizzato dal responsabile del trattamento seguendo le regole e le istruzioni impartite; mantenere la comunicazione con il responsabile del trattamento per risolvere ogni problema che si dovesse presentare nel corso del trattamento.

Inoltre devono essere preventivamente individuati per iscritto i responsabili della custodia della copia delle credenziali utilizzate dagli incaricati del trattamento, che ne garantiscano la riservatezza, nonché le misure organizzative con le quali il titolare possa assicurare la disponibilità dei dati, 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. I custodi devono informare tempestivamente l'incaricato dell'intervento effettuato.

La distribuzione organizzativa dei compiti e delle responsabilità

Il presente atto individua le competenze del titolare, designa i soggetti responsabili del trattamento e definisce i criteri generali da rispettare nell'individuazione dei soggetti incaricati a compiere le operazioni di trattamento.

Il titolare – Funzioni

Ai sensi dell'art. 4, comma 1, lettera f) e dell'art. 28 del Codice, il titolare dei trattamenti di dati personali è quindi l'Azienda U.S.L. di Parma a cui spetta l'adozione degli atti contenenti le scelte di fondo in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Spetta pertanto in particolare all'Azienda U.S.L, nella persona del Direttore Generale:

a. adottare con proprio atto, aggiornandolo periodicamente, il Documento Programmatico per la Sicurezza previsto dall'art. 34, lettera g) del Codice e riferire della sua adozione nella relazione accompagnatoria del bilancio di esercizio;
b. designare il Responsabile della sicurezza;
c. designare il Coordinatore del diritto di accesso dell'interessato ai propri dati personali;
d. designare altri soggetti quali responsabili del trattamento di dati personali, oltre ai soggetti già designati con il presente atto;
e. vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza, e sul rispetto delle proprie istruzioni. Tali verifiche saranno effettuate tramite i responsabili dei trattamenti ed il Responsabile della Sicurezza.

Spetta al Direttore Generale, quale legale rappresentante dell'ente, la sottoscrizione degli atti di notifica, delle comunicazioni e delle richieste al Garante per la protezione dei dati personali (di seguito indicato come Garante). Tale funzione è delegabile ai soggetti designati quali responsabili del trattamento di dati personali.

La funzione relativa alla sottoscrizione del consenso, richiesto da soggetti privati che trattano i dati dell'Azienda SUL di Parma, è direttamente attribuita ai soggetti designati quali responsabili del trattamento di dati personali.

I Responsabili del trattamento di dati personali – Designazione e compiti

Ai sensi dell'art. 4, comma 1, lettera g) e dell'art. 29 del Codice, il responsabile del trattamento di dati personali è il soggetto preposto dal titolare al suddetto trattamento tramite designazione, specificando analiticamente per iscritto i compiti che gli sono affidati.

Nel presente documento sono identificati quali responsabili del trattamento di dati personali i Responsabili di Struttura Complessa come da allegato n.11

I compiti affidati ai responsabili del trattamento sono i seguenti:

a. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento, con particolare riguardo al principio di necessità di cui all'art. 3 del Codice, sia relativamente ai trattamenti già in essere che ai nuovi trattamenti;
b. disporre, in conseguenza alla verifica di cui alla lettera a), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c. vigilare, per conto del Titolare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, secondo le modalità del presente regolamento e segnalando eventuali problemi al responsabile della sicurezza e, in ultima istanza, al Titolare;
d. aggiornare periodicamente l'elenco dei trattamenti di dati personali effettuati dalla struttura di riferimento, anche al fine di garantire un tempestivo aggiornamento del Documento Programmatico per la Sicurezza;
e. predisporre il completamento dell'informativa di cui all'art. 13 del Codice e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
f. individuare gli incaricati del trattamento dei dati personali e fornire agli stessi istruzioni per il corretto trattamento dei dati stessi, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata secondo quanto stabilito dal presente documento e , in particolare, le istruzioni devono quanto meno contenere l'espresso richiamo alle linee guida aziendali per la protezione dei dati personali;
g. predisporre ogni adempimento organizzativo necessario per garantire agli interessati il diritto di accesso ai propri dati personali, secondo quanto stabilito dagli artt. 7 e ss. del Codice;
h. provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati per l'esercizio del diritto di accesso;
i. provvedere direttamente al riscontro nei seguenti casi: qualora l'istanza dell'interessato sia volta ad ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, secondo quanto previsto dal comma 3, lettera b) dell'art. 7 del Codice; qualora si tratti di opposizione al trattamento, secondo quanto previsto dal comma 4 dell'art. 7 del Codice e qualora occorra prorogare il termine per il riscontro, previa comunicazione all'interessato nel caso di richiesta di particolare complessità o per altro giustificato motivo, secondo quanto previsto dal comma 3 dell'art. 146 del Codice;
j. disporre l'adozione dei provvedimenti imposti dal Garante quale misura conseguente all'accoglimento delle richieste degli interessati;
k. predisporre la documentazione e gli atti necessari per il Garante nei casi e nei modi previsti dalla legge;
l. comunicare al Coordinatore del diritto di accesso dell'interessato ai propri dati personali l'individuazione dei responsabili esterni;
m. collaborare con il Responsabile della sicurezza e con il Coordinatore del diritto di accesso dell'interessato ai propri dati personali;
n. individuare i soggetti che effettuano il trattamento dei dati quali incaricati, specificando anche le relative istruzioni. Devono essere designati quali incaricati, qualora effettuino operazioni di trattamento, non soltanto i dipendenti a tempo indeterminato o determinato, ma anche gli altri soggetti

che, ad altro titolo, operano sotto la diretta autorità del Titolare o del Responsabile del trattamento, quali, ad esempio, i lavoratori con contratto di somministrazione di lavoro a tempo determinato,i collaboratori a progetto, i tirocinanti, individuando il profilo d'accesso individuale alle varie banche dati.

I responsabili esterni – Designazione, individuazione e compiti

Si ritiene opportuno stabilire che siano designati, di norma, quali responsabili del trattamento di dati personali, i soggetti esterni all'amministrazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare. A riguardo vedasi l'allegato n.12 "Elenco Responsabili esterni".

Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Per poter operare tale valutazione, occorre quindi specificare già nelle procedure di selezione del bando di gara e del capitolato d'appalto che l'incarico ricomprende anche la designazione a responsabile del trattamento di dati personali.

Tale designazione deve essere effettuata direttamente in convenzione, nel contratto, nel verbale di aggiudicazione o nel provvedimento di nomina tramite:

a. l'indicazione nominativa qualora al trattamento di dati personali siano preposte persone fisiche;
b. l'individuazione della persona giuridica qualora al suddetto trattamento sia preposta una persona giuridica;
c. l'individuazione della pubblica amministrazione o di qualsiasi altro ente qualora al trattamento siano preposti rispettivamente una pubblica amministrazione o qualsiasi altro ente;
d. l'individuazione di una o più persone fisiche qualora, nei sopra riportati casi di cui alle lettere b) e c), il trattamento di dati personali riguardi esclusivamente un settore specifico e limitato dell'ente.

Qualora i soggetti esterni siano persone fisiche ed operino sotto la diretta autorità di un responsabile del trattamento, le stesse devono essere individuate quali incaricati del trattamento.

I compiti affidati ai responsabili esterni del trattamento di dati personali sono i seguenti:

a. adempiere all'incarico attribuito adottando idonee e preventive misure di sicurezza, con particolare riferimento a quanto stabilito dal Codice, dall'Allegato B del Codice, dalle linee guida aziendali in materia di protezione dei dati personali e dalle eventuali disposizioni esplicitate

nell'incarico.
b. predisporre, qualora l'incarico comprenda la raccolta di dati personali, l'informativa di cui all'art. 13 del Codice e verificare che siano adottate le modalità operative necessarie perché la stessa sia effettivamente portata a conoscenza degli interessati;
c. a fronte di eventuali richieste verbali ai sensi dei commi 1-2 dell'art. 7 del Codice, dare direttamente riscontro oralmente, anche tramite propri incaricati secondo le modalità impartite dal Coordinatore del diritto d'accesso;
d. trasmettere, con la massima tempestività, le istanze dell'interessato per l'esercizio dei diritti di cui agli artt. 7 e ss. del Codice che necessitino di riscontro scritto/orale al responsabile del trattamento, per consentire allo stesso di dare riscontro all'interessato nei termini stabiliti dal Codice;
e. fornire al responsabile del trattamento la massima assistenza, necessaria per soddisfare tali richieste, nell'ambito dell'incarico affidatogli;
f. individuare gli incaricati del trattamento dei dati personali e fornire agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; le istruzioni devono quanto meno contenere l'espresso richiamo alle linee guida aziendali in materia di protezione dei dati personali;
g. attestare, qualora l'incarico affidato ricomprenda l'adozione di misure minime di sicurezza, la conformità degli interventi alle disposizioni di cui alla misura 25 dell'Allegato B del Codice e trasmettere tale attestazione al Responsabile della sicurezza.

Tali compiti possono essere ulteriormente precisati e, qualora fosse necessario, adattati alla natura dello specifico incarico comportante il trattamento di dati personali attribuito al soggetto esterno. Le specificazioni e/o gli adattamenti devono essere analiticamente stabiliti in convenzione, nel contratto o nel provvedimento di nomina.

Il Responsabile della sicurezza

Il Codice impone, in particolare al Titolo V, numerosi obblighi in materia di sicurezza dei dati e dei sistemi.

Si reputa opportuno, in ragione sia della complessità organizzativa della Azienda U.S.L. di Parma sia della peculiarità della materia, che richiede particolari competenze professionali anche tecniche, designare un soggetto con la specifica responsabilità di operare per la sensibilizzazione, il coordinamento, la vigilanza e l'applicazione di tali obblighi, secondo i compiti di seguito definiti.

Al Responsabile della sicurezza dell' Azienda U.S.L. sono affidati i seguenti compiti:

a. curare la redazione e l'aggiornamento del Documento Programmatico per la Sicurezza relativamente all'ambito dell'Azienda U.S.L. di Parma;
b. collaborare con il Titolare per definire linee guida in materia di protezione dei dati personali;

c. curare la redazione di eventuali disciplinari tecnici da sottoporre all'approvazione del Direttore Generale, promuovendone anche l'aggiornamento ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
d. curare la redazione del Regolamento per l'utilizzo degli strumenti informatici dell'Azienda U.S.L. di Parma relativo alle modalità e alle procedure per l'effettuazione di controlli sull'utilizzo delle strumentazioni informatiche;
e. attivarsi ogni qualvolta venga avvertito un problema di sicurezza per:
- verificare il rispetto delle misure minime di sicurezza;
- individuare, se necessario, altre misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali;
- inviare opportuna segnalazione in prima istanza ai Responsabili dei trattamenti e in ultima istanza al Titolare, affinché pongano in essere le misure necessarie per garantire la sicurezza dei dati;

f. individuare le misure idonee da osservare nell'esecuzione dei trattamenti dei dati personali aggiornandole in relazione all'evoluzione della tecnica, della normativa e dell'esperienza, segnalando eventuali problemi rilevati in prima istanza ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;
g. vigilare per conto del Titolare, anche tramite verifiche periodiche, sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e al rispetto delle proprie istruzioni, segnalando eventuali problemi rilevati, in prima istanza, ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;
h. promuovere l'istruzione e la formazione, in collaborazione con il Servizio preposto, dei Responsabili e degli Incaricati dei trattamenti dei dati personali ivi compresi gli incaricati nominati da responsabili esterni ma operanti sotto la diretta autorità del Responsabile interno del trattamento, con particolare riferimento all'adozione e all'osservanza delle singole misure di sicurezza;
i. promuovere, in collaborazione con il Servizio preposto, la cultura della sicurezza anche attraverso un piano di comunicazione e divulgazione all'interno dell' Azienda;
j. raccogliere e conservare ai fini di eventuali verifiche, le attestazioni di conformità alle disposizioni della misura 25 dell'Allegato B del Codice.

<u>Il Coordinatore del diritto di accesso dell'interessato ai propri dati personali</u>

Il Codice, agli artt. 7 e ss., attribuisce agli interessati il potere di esercitare, sui propri dati personali, un diritto di accesso, relativo sia alla conoscenza dei dati stessi che ad un intervento (ad es., di integrazione o cancellazione).

L'art. 10, comma 1, lettera b) del Codice, stabilisce inoltre che il titolare è tenuto ad adottare idonee misure volte, in particolare, a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

Si reputa quindi opportuno, in ragione della complessità organizzativa dell'Azienda U.S.L. di Parma, designare un soggetto con la specifica responsabilità di operare per la sensibilizzazione e il coordinamento di tale diritto, denominandolo "Coordinatore del diritto di accesso dell'interessato ai propri dati personali".

Al Coordinatore del diritto di accesso dell'interessato ai propri dati personali dell' Azienda U.S.L. di Parma, sono affidati i seguenti compiti:

a. promuovere il coordinamento e la sensibilizzazione dei Responsabili e degli incaricati del trattamento dei dati, sia in via generale e preventiva che su singola richiesta, sui diritti di cui all'art. 7 e ss. del Codice, sul loro contenuto, sulla loro applicazione e sulle modalità di ottemperanza alle richieste dell'interessato;
b. collaborare con il Titolare per definire linee guida in materia di protezione dei dati personali relativamente al diritto di accesso agli stessi dati da parte dell'interessato;
c. collaborare con i singoli interessati, anche fornendo istruzioni sul contenuto dei diritti di cui all'art. 7 del Codice e sulla procedura per il loro esercizio, alla redazione e compilazione delle istanze per l'esercizio dei diritti medesimi;
d. smistare le singole istanze verso i Responsabili del trattamento, responsabili anche del riscontro e competenti ad ottemperare alle medesime istanze;
e. vigilare, per conto del Titolare, sul puntuale e corretto invio del riscontro, segnalando eventuali problemi rilevati, in prima istanza, ai Responsabili dei trattamenti di dati personali e, in ultima istanza, al Titolare;
f. proporre l'adozione delle singole misure ritenute opportune per agevolare l'accesso ai dati personali da parte dell'interessato, coordinandosi con i Responsabili del trattamento e proporre le misure opportune per semplificare le modalità di accesso e per ridurre i tempi di attesa, indicandole, laddove necessario, ai Responsabili del trattamento e al Responsabile della sicurezza;
g. curare la pubblicazione e il relativo aggiornamento dell'elenco dei responsabili esterni, in base alle comunicazioni effettuate dai Responsabili del trattamento;
h. individuare e promuovere, in collaborazione con il Responsabile della sicurezza, le misure idonee a garantire l'esercizio dei diritti di cui all'art. 7 del Codice, anche mediante software che consentano il facile, agevole e approfondito reperimento di tutti i dati personali trattati in forma elettronica nell'ambito dell'Azienda U.S.L. di Parma;
i. promuovere l'istruzione e la formazione, in collaborazione con il Servizio preposto, dei Responsabili e degli Incaricati dei trattamenti dei dati personali, con particolare riferimento all'osservanza delle procedure da adottare per favorire l'esercizio del diritto di accesso degli interessati ai propri dati personali;
j. promuovere, in collaborazione con il Servizio preposto e con il Responsabile della sicurezza, la cultura sui diritti dell'interessato, anche attraverso un piano di comunicazione e divulgazione all'interno dell'Ente;
k. proporre l'adozione di ogni altro provvedimento e adempimento necessario per la corretta applicazione dell'art. 7 e ss. del Codice.

Gli incaricati – Criteri generali per l'individuazione delle persone fisiche e per le istruzioni da impartire alle stesse

L'art. 4, lettera h) e l'art. 30 del Codice stabiliscono che il titolare o il responsabile devono designare, quale incaricati del trattamento di dati personali, le persone fisiche che effettuano le operazioni di trattamento, operando sotto la loro diretta autorità.

Devono pertanto essere designati quali incaricati, qualora effettuino operazioni di trattamento, non soltanto i dipendenti a tempo indeterminato o determinato, ma anche gli altri soggetti che, ad altro titolo, operano sotto la diretta autorità del Titolare o del Responsabile del trattamento, quali, ad esempio, i lavoratori con contratto di somministrazione di lavoro a tempo determinato,i collaboratori a progetto, i tirocinanti, individuando il profilo d'accesso individuale alle varie banche dati.

Il Codice specifica inoltre che la designazione:

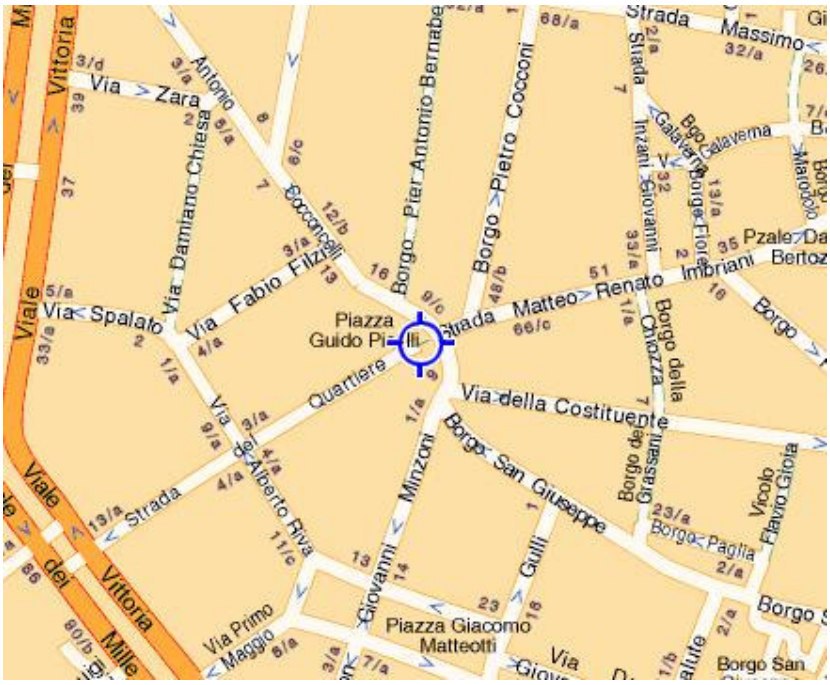
a. deve essere effettuata per iscritto, individuando puntualmente l'ambito del trattamento consentito;
b. è considerata quale designazione anche la documentata preposizione della persona fisica ad una unità organizzativa per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

I Responsabili del trattamento, devono pertanto designare/revocare per iscritto i soggetti autorizzati ad effettuare le operazioni di trattamento e darne tempestiva comunicazione, per gli adempimenti di competenza, al Responsabile della Sicurezza. La designazione deve essere aggiornata almeno annualmente.

La gestione degli incaricati, dei responsabili, dei trattamenti e di tutto ciò che ruota attorno alla sicurezza inclusa la formazione degli operatori non è cosa semplice ed immediata. A tal ragione l'Azienda USL di Parma ha deciso di adottare un sistema software chiamato **IntranetDPS**. Tale software permette di gestire, e di far gestire ai diretti interessati, tutte le operazioni per una corretta manutenzione del processo di assegnazione responsabili ed incaricati. Ognuno per il suo ruolo gestirà quanto di pertinenza ossia il Servizio RIT potrà inserire i trattamenti aziendali e non, fornirà supporto di assistenza ai diversi operatori, stilerà le informazioni inerenti i macchinari utilizzati nella gestione dei trattamenti. I responsabili delle strutture individueranno gli incaricati dei trattamenti e gli notificheranno tramite lettere di incarico il loro ruolo. La stretta collaborazione tra i titolari dei servizi ed il personale del servizio informatico, costituisce la base essenziale per un corretto mantenimento delle informazioni. Tali informazioni devono essere veicolate dalle zone periferiche della struttura aziendale al centro informatico, essendo queste la parte attiva dei servizi.

Sistema Informatico

Viene riportata di seguito la locazione fisica del Servizio RIT e della sala server:



Le misure di sicurezza sono articolate in gruppi correlati:

- le minime indicate dal Codice (artt. 33, 34, 35 e 36) e integrate dal Disciplinare tecnico (punti da 1 a 29);

- le misure c.d. idonee (art. 31) decise in autonomia dal titolare in relazione alle proprie specificità.

Per “misure minime” si intende il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 (comma 3, lettera a).

Per "strumenti elettronici" si intendono gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento (art. 4, comma, 3 lettera b).

L'art. 31 prescrive l'obbligo della sicurezza a cui tutti devono attenersi e individua i principi fondamentali della "custodia" e del "controllo". I dati personali oggetto di trattamento devono essere custoditi e controllati durante tutto il ciclo di vita del trattamento.

La custodia e il controllo non sono misure immutabili, ma anzi devono essere

adeguate in relazione alle conoscenze acquisite ed all'evolversi della tecnologia.

I parametri di custodia e controllo variano sia in relazione alla natura dei dati trattati (dati personali, sensibili o giudiziari, nelle accezioni indicate dal Codice stesso), sia in funzione delle caratteristiche del trattamento, cioè delle modalità con cui viene svolto. A tal fine il disciplinare tecnico distingue fra trattamenti con strumenti elettronici e trattamenti senza l'ausilio di strumenti elettronici.

Mediante l'adozione preventiva di idonee misure di sicurezza si mira a raggiungere il fine ultimo della custodia e del controllo ossia la riduzione dei rischi quali:

- l
a distruzione o perdita, anche accidentale dei dati stessi;
- l
'accesso non autorizzato o il trattamento non consentito o non conforme ai fini per i quali i dati sono raccolti.

Nel primo caso valgono le regole indicate nel disciplinare tecnico nei punti da 1 a 26, nel secondo caso quelle indicate nei punti da 27 a 29.

Gli obblighi di sicurezza riguardano chiunque e, più in specifico, il "titolare" del trattamento, il "responsabile", e gli "incaricati". Le definizioni di "titolare" e "responsabile" contenute nel Codice sono simili a quelle precedenti e conservano l'inciso "ivi compreso il profilo della sicurezza".
La compilazione del Documento programmatico sulla sicurezza era una misura prevista all'art. 6 del D.P.R. 28 luglio 1999, n. 318.
Con la nuova norma contenuta nel Codice alla lettera g), comma 1 dell'art. 34, insieme alle dettagliate prescrizioni di cui ai punti 19 e 26 del Disciplinare tecnico, il documento assume una rilevante importanza nella pianificazione di ogni scelta di sicurezza ed il titolare deve riferire nella relazione accompagnatoria del bilancio di esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento come richiesto dalla legislazione vigente.

Il DPS ha il compito di definire gli standards comportamentali e tecnologici che garantiscano l'adeguatezza ed il buon uso del sistema di sicurezza dell'azienda sanitaria, al fine di prevenire accessi non autorizzati ed utilizzi impropri delle informazioni.
Tali standard, definiti conseguentemente e in coerenza con le Politiche di Sicurezza aziendali, sono necessari per precisare e dettagliare le direttive ivi contenute, oltre che per aggiornare dinamicamente le misure di sicurezza a seguito dei cambiamenti nei sistemi AUSL e dell'evoluzione della tecnologia e della conoscenza.
Il presente Piano per la Sicurezza costituisce la raccolta delle regole e standards aziendali in fatto di sicurezza. Si veda il Regolamento di cui all'allegato n.15
Per Sicurezza si intende una combinazione delle proprietà di Riservatezza, Integrità e Disponibilità di un sistema o di un prodotto. Le funzioni di sicurezza necessarie per garantire tali proprietà sono generalmente raggruppabili all'interno delle seguenti aree:

- Sicurezza Organizzativa
- Sicurezza Fisica
- Sicurezza Logica
- Piano di Continuità Operativa

Si sottolinea fin d'ora che gli aspetti della Sicurezza Organizzativa sono essenziali sia per la Sicurezza Fisica che per la Sicurezza Logica

Per poter applicare idonee misure di sicurezza è necessario effettuare l'Analisi dei Rischi a cui sono esposti i trattamenti dei dati.

Analisi dei Rischi

L'analisi dei rischi costituisce la fase di partenza dell'attività di progettazione del piano aziendale della sicurezza ed è un elemento fondamentale del documento programmatico della sicurezza. Gli obiettivi principali dell'analisi sono:

- Avere la visibilità di esposizione al rischio del patrimonio informativo;
- Avere una mappa delle contromisure di sicurezza .

A tal fine, è indispensabile:

- l'individuazione degli elementi del sistema informativo automatizzato e non;
- un censimento delle principali risorse di elaborazione (soprattutto server), degli applicativi e delle banche dati.

Risorse Hardware Rientrano in questa categoria le workstations, le stampanti, i server, i router, gli switch i dischi e tutte le apparecchiature di comunicazione. Le principali minacce di questi dispositivi sono i malfunzionamenti causati da guasti tecnici, eventi naturali, sabotaggi od intercettazioni. Quest'ultima eventualità interessa principalmente i server e la rete in generale. Occorre quindi attuare contromisure al fine di evitare intrusioni o monitoraggi indebiti.

Risorse Software Esse sono rappresentate dai sistemi operativi, software applicativi o di base, tutte le basi dati, e tutto ciò che può essere fatto “girare” su di un elaboratore. Le minacce che incombono su queste risorse sono diverse e spaziano dall'errore di sviluppo, che favorisce intrusioni, ad attacchi veri e propri portati dall'esterno via rete, o direttamente dall'interno tramite codice malicius.

Dati Con tale termine s'intende il contenuto degli archivi cartacei od elettronici, delle basi dati, dei file di log, delle copie di salvataggio e di tutto ciò che rappresenta informazione a livello aziendale. Si identificano due principali fonti di rischio e precisamente: quella dell'accesso non autorizzato ai dati e quella che comprende una volontà precisa di arrecare danno.

Le Risorse professionali Un elemento da tenere in considerazione per la gestione e l'applicazione della sicurezza è la preparazione professionale degli operatori del settore informatico. Fanno parte di questa categoria gli amministratori di rete e di sistema, i manutentori hardware e software.

Documentazione cartacea Tutto ciò che riguarda la documentazione dei software, delle installazioni Hardware, delle procedure. Tali elementi sono soggetti al rischio di accesso e trattamento non autorizzato delle informazioni in essi contenute.

Supporti di memorizzazione Vengono utilizzati per consentire una salvaguardia sia dei prodotti informatici dell'azienda sia dei dati di controllo (log) o dati procedurali. Come tutti i componenti appartenenti a questa categoria i rischi che incombono sono: il deterioramento nel tempo, l'inaffidabilità del mezzo fisico e, in pospettiva, un avanzamento tale della tecnologia da non consentire il riutilizzo dei supporti.

Classificazione e valutazione dei beni informatici

E' possibile individuare delle categorie di classificazione in base agli elementi di integrità, riservatezza e disponibilità. Per la valutazione dei beni sono disponibili diverse metodologie, alcune delle quali basate su principi quantitativi (costo di ripristino, costi di elaborazione tramite risorse alternative, ecc), altre su principi qualitativi (interruzione di servizi, violazione aspetti legislativi, perdità di operatività, ecc).
Di seguito vengono elencati i documenti relativi all'analisi dei rischi dei principali settori informatici.

Tipo	***Nome documento***
Server	T0201 Allegato n.4
Workstations	T0202 Allegato n.5
Reti	T0203 Allegato n.6
Applicativi	T0204 Allegato n.7
Misure	T0205 Allegato n.8

Misure in essere e da adottare

1. Sicurezza Organizzativa

Il processo della sicurezza dei sistemi informativi automatizzati richiede che, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo medesimo.
Gli aspetti organizzativi della sicurezza dei sistemi informativi automatizzati riguardano principalmente:

- la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo sicurezza;
- l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

In particolare modo si intende dar rilievo alle procedure da adottare, nel metodo, dell'attivazione di connessioni verso i server aziendali da esterni, da interni e le misure da adottare per ridurre al minimo anomalie o manomissioni. In particolare si possono redigere alcune linee di massima per la messa opera per l'accesso ai servizi.

Richiesta di accesso ai trattamenti
I responsabili dei trattamenti dei dati, individuati dall'azienda tramite delibera, personalmente o loro delegati tramite il software **IntranetDPS** possono richiedere le credenziali di accesso per i loro incaricati una verificata la corrispondenza tra le mansioni svolte dal richiedente e la tipologia di trattamento richiesto.
In caso di revoca di una designazione, il responsabile del trattamento deve farne espressa comunicazione al servizio informatico sempre utilizzando il software sopra citato.

Gestione dei dati di accesso al trattamento
Il titolare, il responsabile o l'incaricato hanno l'obbligo di tenere riservate le proprie credenziali di accesso al trattamento non facendone comunicazione ed attenendosi alle regole regole citate all'allegato 1.

2. Sicurezza Fisica

Lo scopo delle procedure per la sicurezza fisica è quello di garantire chi opera sui sistemi informatici in merito alla loro integrità sia nell'area di operazioni sia nell'utilizzo della componentistica hardware. A tale scopo vengono stilate le contromisure che possono essere ricondotte fondamentalmente alle due seguenti categorie.

a) Sicurezza di area
La sicurezza di area mira a prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza della *sale macchine* rispetto a danneggiamenti accidentali o intenzionali, nonché alla protezione fisica dei supporti. A tal fine:

- Il locale è chiuso, anche se presidiato;
- Accesso a locali 'delicati' tramite riconoscimento elettronico;
- L'accesso è consentito solo alle persone autorizzate;
- I visitatori occasionali devono essere accompagnati;

b) Sicurezza delle apparecchiature hardware
La sicurezza delle apparecchiature è riconducibile da un lato alle protezioni da danneggiamenti accidentali o intenzionali e dall'altro alla sicurezza degli impianti di

alimentazione e di condizionamento. Anche la manutenzione dell'hardware rientra in questa area, come anche la protezione da manomissione o furti.
Le apparecchiature informatiche per l'erogazione del servizio sono conservate in aree ad accesso controllato, dotate di impianto di rilevazione antincendio e di gruppi di continuità elettrica.

3. Sicurezza Logica

La sicurezza logica è una componente particolarmente critica della Sicurezza del Sistema Informativo. Il campo di applicazione della Sicurezza Logica riguarda principalmente la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.
Le contromisure di Sicurezza Logica sono quindi da intendersi come l'insieme di misure di *sicurezza di carattere tecnologico e di natura procedurale ed organizzativa* che concorrono nella realizzazione del livello di sicurezza da raggiungere. Diamo di seguito alcune indicazioni inerenti l'identificazione e l'autorizzazione.
Si possono considerare diversi livelli di sicurezza classificandoli in base alle tipologie di utilizzo. In generale devono essere valide queste regole sia che avvenga un'autenticazione lato utente che direttamente da un server. Queste politiche di sicurezza vanno sotto il nome di "controllo degli accessi", che consiste nel garantire che tutti gli accessi agli oggetti del sistema informativo avvengano esclusivamente secondo modalità prestabilite. Si rende indispensabile prevedere un meccanismo che costringa ogni utente ad autenticarsi (cioè dimostrare la propria identità) prima di poter accedere al sistema. Il meccanismo sinora più usato a tale scopo è quello delle password.
Se il sistema di accoglienza lo consente è consigliato l'uso di messaggistica di accoglienza (banner di log-in) per ricordare all'utente che sta entrando in una rete protetta.
In definitiva il controllo accessi può essere visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione).

L'autenticazione e l'accesso ai sistemi informatici avviene dopo il valido riconoscimento delle credenziali "utente" tramite il "login", il quale deve essere sottoposto a diversi criteri:

- User-id: Lo user-id deve poter essere riconducibile ad un singolo individuo a cui è stato assegnato e che ne è il responsabile della custodia.
- Password: L'utente deve conservare con estrema cura la password di accesso ai sistemi, ha l'obbligo di non comunicarla ad altri e di sostituirla immediatamente in caso di sospetta diffusione. La password deve essere cambiata almeno ogni tre mesi. Alcune regole per la creazione delle password possono essere visionate nell'allegato 1.
- Revoca delle User-id : Quando un utente non ha più la necessità di accedere ad una banca dati, lascia l'azienda o quando vengono a cadere le motivazioni che danno diritto di accesso al sistema informativo aziendale, la sua utenza deve essere disabilitata. Il Responsabile del servizio dell'interessato o colui che aveva richiesto l'utenza deve richiederne la disabilitazione.
- Sostituzione immediata delle password iniziali: Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione o al primo utilizzo.
- Ripristino della password: La richiesta di ripristino della password viene effettuata dall'interessato tramite comunicazione (email, fax,..) al servizio competente. L'operatore del servizio competente, previa identificazione dell'utente richiedente, provvede al ripristino della password e ne dà comunicazione al diretto interessato.

Quanto sopra vale per autenticazioni interne alla rete, in cui viene garantito un certo grado di sicurezza.
Per connessioni esterne all'azienda occorre prevedere un controllo più accurato attraverso un sistema di “autenticazione forte”:

- Autenticazione accessi da Internet**:** Si deve prevedere il superamento dell'utilizzo della modalità userid/password poiché non forniscono sufficienti garanzie di sicurezza per le connessioni ai sistemi aziendali da internet o in dial-up. La positiva identificazione degli accessi da internet può essere garantita solamente da una autenticazione forte, preferibilmente basata su certificato digitale e smartcard, usando i meccanismi di sfida/risposta (challenge/response). Questo meccanismo consente l'identificazione certa dell'utente e del server poiché instaura una comunicazione cifrata (secure-messaging) e garantisce dall'attacco dell' "uomo-nel-mezzo", ossia che una terza persona si intrometta nella comunicazione alterandola o compromettendone l'integrità.

- Autenticazione del Server: Avviene attraverso l'uso del certificato digitale usato dal server per presentarsi al browser. L'instaurarsi della sessione https (ssl2) dà garanzia all'utente che i dati che sta ricevendo sono certamente quelli dell'AUSL. Questa modalità garantisce l'integrità del dato all'utente finale.

- Autenticazione del Client: Avviene attraverso l'uso del certificato digitale utente da parte del browser. L'instaurarsi della sessione https (ssl3) , aggiunge alla situazione precedente la garanzia dell'identità utente. Questa modalità garantisce sia l'integrità del dato che l'identità dell'utente connesso.

Questi due ultimi tipi di autenticazione forniscono un diverso livello di sicurezza e sono da valutare quando si realizzano collegamenti alle applicazioni AUSL tramite internet. La scelta della modalità di autenticazione non può prescindere dalla natura delle informazioni trattate e dalla operatività dell'applicazione.

Al fine di garantire la tracciabilità delle operazioni effettuate sulle macchine aziendali si rende necessaria una politica di controllo basata sui log, generati da applicazioni, da sistemi di base o di rete.

- Logs richiesti alle applicazioni che trattano dati critici: Tutte le applicazioni in produzione che trattano dati critici devono generare logs che consentano di tracciare ogni modifica, aggiunta o cancellazione delle informazioni.

- Inclusione di eventi rilevanti per la sicurezza nei logs di sistema: I sistemi in produzione ritenuti critici per l'azienda, devono generare dei logs di tutti gli eventi rilevanti ai fini della sicurezza, ad esempio, tentativi di accesso con password errata, tentativi di utilizzare privilegi non assegnati, modifiche alla configurazione delle applicazioni o dei sistemi.

- Tracciabilità per tutti i comandi privilegiati di sistema: Tutti i comandi effettuati dall'operatore di sistema devono essere tracciati e riconducibili al operatore che gli ha effettuati.

- Contenuti minimi dei logs di produzione:

  - Attività della sessione utente(userid, timestamp del login e del logout, applicazioni usate).
  - Cambiamenti alle informazioni critiche della applicazione(dati di configurazione).
  - Modifiche ai privilegi utente.

- Periodo di conservazione dei logs: I logs contenenti informazioni relative agli eventi rilevanti per la sicurezza devono essere conservati per almeno 3 mesi e secondo modalità che garantiscano la non modificabilità. Potranno essere letti solo da persone autorizzate. Sono particolarmente importanti per la determinazioni di errori, diagnosi su

falle del sistema di sicurezza,ed eventuali verifiche legali.

Trattandosi di direttive di ordine generale, sarà compito del responsabile di ogni applicativo e del responsabile di sistema, realizzare e verificare il rispetto di tali politiche.

- Protezione alla disattivazione, modifica, o cancellazione dei log: Il meccanismo di registrazione degli eventi relativi alla sicurezza deve essere resistente agli attacchi. Questi includono i tentativi di disattivare, modificare o cancellare i meccanismi per la registrazione o i log stessi.
- Persone autorizzate ad esaminare i logs: Tutti i log di sistema e di applicazione devono essere conservati in maniera tale da non poter essere facilmente letti da personale non autorizzato. Una persona non è autorizzata alla lettura se non appartiene a strutture di sicurezza informatica, sistemistiche o in generale non rientra tra i suoi specifici compiti.
- Riesame dei logs di sistema: Per consentire appropriate azioni correttive è necessario predisporre regolari attività di riesame dei log relativi agli eventi di sicurezza.
- Notifica agli utenti del logging: Gli utenti devono essere informati sulle azioni che costituiscono violazioni di sicurezza e, devono altresì essere informati, che tali violazioni saranno loggate.

3.1.Protezione contro attacchi esterni

Antivirus

I virus informatici, indicati con il termine generico di "malicius code" (codice maligno – programma dannoso), sono i rappresentanti più noti di una categoria di programmi scritti per generare intenzionalmente una qualsiasi forma di danneggiamento ad un computer o ad una rete.
La miglior difesa contro i virus informatici consiste nel definire un'architettura antivirus composta da regole comportamentali e da procedure operative, a protezione dell'intero sistema informatico.
Tutti gli utenti del sistema sono tenuti a conoscere e rispettare tali regole e, l'amministratore di sistema, è tenuto a mantenere costantemente operative e aggiornate le procedure software predisposte.
A tal fine, tali procedure hanno la caratteristica di mantenere automaticamente aggiornati i pattern di controllo, sia sui server che sulle stazioni client.
E' possibile verificare che ogni stazione dotata di antivirus utilizzi il pattern aggiornato mantenendo attiva l'opzione di aggiornamento automatico.

Utilizzo di internet

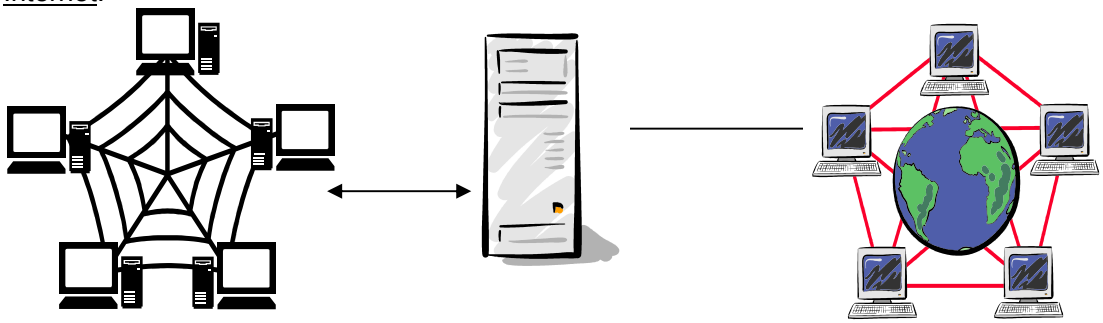
La *"Internet Acceptable Usage Policy – IAUP"*, viene ormai sentita come una esigenza comune in diverse organizzazioni che abbiano una presenza o una connessione verso Internet poiché con questa politica è possibile stabilire i criteri e le regole per l'accesso ai sistemi informativi aziendali sia per utenti esterni che utenti facenti parte dell'organizzazione stessa.
In aggiunta si definisce anche la regolamentazione dell'accesso da parte degli utenti interni ai sistemi presenti sulla public-Internet. La connessione verso Internet attribuisce all'utente la responsabilità di rappresentare l'organizzazione rispetto ad Internet, per esempio nello scambio di messaggi di posta elettronica. Ci si aspetta in tal senso che l'utente utilizzi Internet per fini legittimi ed in linea con il business della propria azienda.
Il disegno di una politica per un utilizzo accettabile e appropriato di Internet (IAUP) delinea le aspettative di una organizzazione rispetto ad un utilizzo di questa risorsa: l'Azienda richiede che i propri dipendenti accedano ad Internet al solo fine di attività di lavoro e attraverso le sole infrastrutture appositamente predisposte, secondo i criteri di sicurezza definiti e nella piena legalità.
Un utilizzo appropriato di Internet deve tenere conto delle disposizioni e delle indicazioni che emergono in questi tre ambiti:

- Aziendale: la navigazione in Internet ha un costo aziendale (risorse umane, di rete, sistemi) per cui ne è consentito l'uso solo per motivi di lavoro e con le finalità proprie della propria attività professionale.
- Internet: la "comunità Internet" ha redatto un documento (RFC 1855), che delinea un set minimo di linee guida per il "comportamento in rete" (Netiquette, Network Etiquette - allegato 2).
- Legislativo: Il comportamento dell'utente è soggetto alle disposizioni vigenti, in particolare alla legge 547 del 23 Dicembre 1993 redatta in materia di reati informatici ed al d.lgs 196/2003 ed alla legge sul diritto d'autore.

3.2 Configurazione della rete.

Basandoci su un classico schema a blocchi diamo una sintetica descrizione dello schema fisico della rete aziendale.

Internet:



Il collegamento tra l'azienda USL con altre reti non fidate (ad esempio Internet) deve essere protetto da un sistema antintrusione denominato Firewall. Nel caso in esame utilizziamo un proxy che funge da filtro per le chiamate in entrata ed in uscita dalla rete interna.
Vanno delineate alcune regole al fine di evitare intrusioni indesiderate :

- tutto il traffico deve passare per il Proxy;
- solo il traffico autorizzato dal servizio può transitare per il Firewall;
- l'integrità del Firewall da accessi esterni non conformi alle regole definite sarà periodicamente verificata tramite auditing esterno;

Trasmissione di informazioni riservate: Il passaggio di informazioni riservate da una rete esterna (Internet, collegamento dial-up) deve essere protetto tramite crittografia. In particolare sono riservati i dati user-id e password, ne segue che l'autenticazione via rete deve essere crittografata.

Collegamenti via modem: I collegamenti via modem devono essere strettamente controllati. Tali collegamenti vanno possibilmente raggruppati su un asynchronous communications server, su cui verranno attivati sistemi di autenticazione; l'accesso alle risorse di rete verrà abilitato solo al completamento positivo di tale autenticazione. Dove possibile vanno attivate funzioni di logging. Quando non utilizzati, i modem collegati alle workstation devono restare spenti.
Verifiche e controlli di tali comportamenti saranno svolte nell'ambito delle attività di audit esterno delle rete.

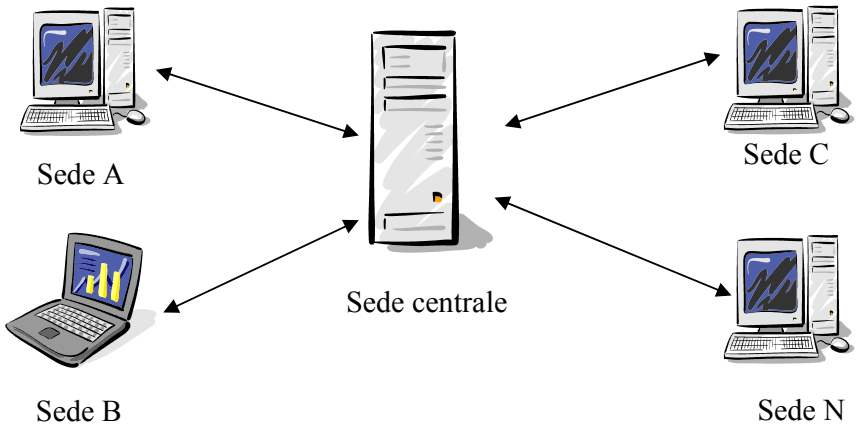
Collegamenti tramite Reverse Proxy

Vista la crescente richiesta dei servizi aziendali da parte di strutture accreditate (farmacie, case di cura, etc...) si è reso necessario alzare il livello di controllo qualitativo del traffico in entrata. Il Reverse Proxy pone una barriera tra ciò che l'azienda può erogare ed il mondo esterno limitando la visibilità della rete aziendale ed aumentando il controllo sulle richieste esterne.

Collegamenti via VPN: è una rete privata instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso come per esempio internet. Lo scopo delle reti VPN è di dare alle aziende le stesse possibilità delle linee private in affitto ad un costo inferiore sfruttando le reti condivise pubbliche.
Le reti VPN utilizzano collegamenti che necessitano di autenticazione per garantire che solo gli utenti autorizzati vi possano accedere, per garantire la sicurezza che i dati inviati in Internet non vengano intercettati o utilizzati da altri non autorizzati, esse utilizzano sistemi di crittografia.
Le reti VPN sicure adottano dunque protocolli che provvedono a cifrare il traffico transitante sulla VPN. Oltre alla cifratura, una VPN sicura deve prevedere nei suoi protocolli dei meccanismi che impediscano violazioni della sicurezza, come ad esempio il furto dell'identità digitale o l'alterazione dei messaggi

Tipo	***Nome documento***
Elenco Connessioni VPN	T0305 Allegato n.17

Intranet:



Trattandosi di connessioni interne, quindi ragionevolmente sicure, il traffico di rete interno non subisce particolari trattamenti di sicurezza se non quelli riconducibili al software utilizzato. Dalla conformità della struttura della rete se ne evince che la comunicazione tra la sede N e la sede C passa sempre per la sede centrale posta presso il Servizio RIT.

Server:

Con il termine server si intendono tutte quelle apparecchiature che forniscono dei servizi. Tali apparati ricoprono un ruolo fondamentale all'interno dell'azienda in quanto rappresentano lo snodo tra il servizio informatico ed i servizi che richiedono accesso alle procedure.

Il personale addetto alla loro attività deve essere in possesso di uno skill altamente qualificato ed il più possibile aggiornato. Tali soggetti sono i responsabili del corretto funzionamento dei server e degli accessi a tali macchine.
Tali operatori vengono identificati all'interno del servizio come 'amministratori di rete'.
Sotto la loro supervisione ricade anche la gestione, manutenzione e sicurezza di tutti gli apparati che costituiscono per intero la rete fisica aziendale come gli switches o similari.

Documenti allegati:

Tipo	***Nome documento***
Linee Trasmissione Dati	T0301 Allegato n.9
Elenco Strutture Aziendali	T0302 Allegato n.10
Elenco Server Aziendali	T0304 Allegato n.15

Sistema di protezione dati (backup)

Un aspetto molto importante della sicurezza dei dati è rappresentato dalla loro conservazione. Il controllo degli accessi alle macchine server è strettamente controllato dalla sicurezza di rete, dalle infrastrutture predisposte nei locali nonchè dai controllo di accesso ai locali stessi. Malgrado tutti i possibili controlli che possono essere messi in opera non vi è nessuna garanzia della conservazione delle informazioni.
Un ulteriore passo per salvaguardare i dati, è quello di predisporre una procedura di backup. In azienda, al momento è predisposta una batteria di nastri che esegue giornalmente il salvataggio dei dati presenti nei server. Si possono ottenere così due livelli di sicurezza in quanto la copia della domenica viene clonata e conservata in cassaforte per un mese.

Conservazione password e chiavi cassaforte

Oltre alle procedure per il controllo della password ed ai normali controlli di accesso ai locali, si sta approntando un'altro grado di protezione al fine di evitare intrusioni o manomissioni: le password di amministrazione delle principali macchine di lavoro dell'azienda verranno singolarmente riposte all'interno di buste sigillate. Tali buste vanno riposte in un apposito luogo ad accesso fortemente ristretto, quale una cassaforte a combinazione o similari. Qualora le esigenze lo rendesse necessario si potranno aprire le buste, previo cambio della password e la sigillazione delle stesse. Stesso discorso vale per le chiavi delle casseforti le quali vanno prelevate la mattina e riposte al termine della giornata lavorativa in un luogo protetto. Resta inteso che qualunque variazione delle password o la scelta del luogo di conservazione va comunicato solo a chi di dovere.

VIDEOSORVEGLIANZA

Con il provvedimento del 29 aprile 2004 il Garante ha specificato in maniera approfondita il provvedimento del 29 novembre 2000 e ha individuato 4 principi da osservare affinchè la videosorveglianza sia legittima: **liceità, necessità, proporzionalità, finalità**.
Il principio di liceità consente la raccolta e l'uso delle immagini qualora esse siano necessarie per adempiere ad obblighi di legge o siano effettuate per tutelare un legittimo interesse. La videosorveglianza è consentita, **senza necessità di alcun consenso**, qualora essa sia effettuata nell'intento di perseguire fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, atti di vandalismo, prevenzione di incendi, sicurezza del lavoro.
Secondo il principio di necessità va escluso ogni uso superfluo ed evitati eccessi e ridondanze nei sistemi di videosorveglianza. La raccolta e l'uso delle immagini deve essere proporzionale agli scopi perseguiti.
Il principio di proporzionalità pur consentendo margini di libertà nella valutazione da parte del titolare del trattamento, non comporta però scelte del tutto discrezionali e insindacabili.
Secondo il principio di finalità gli scopi perseguiti devono essere determinati, espliciti e legittimi. Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza. La videosorveglianza non ha quindi finalità di sicurezza pubblica, prevenzione o accertamento dei reati che competono invece solo ad organi giudiziari o di polizia giudiziaria oppure a forze armate o di polizia.
L'eventuale **conservazione temporanea delle immagini** deve essere commisurata al grado di indispensabilità e per il solo tempo necessario e predeterminato a raggiungere la finalità perseguita. La durata della conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione.
Le ragioni delle scelte di conservazione delle immagini devono essere adeguatamente documentate in un atto autonomo conservato presso il titolare ed il responsabile del trattamento e ciò anche ai fini della eventuale esibizione in occasione di visite ispettive.

Tipo	*Nome documento*
Videosorveglianza	P0104 Allegato n.18

ADDEBITI TELEFONICI

Per quanto concerne la trattazione dei dati sia in formato elettronico che cartaceo del traffico telefonico aziendale si rimanda alla disposizione con protocollo numero 104825/int del 24 Novembre 2006.

ARCHIVIAZIONE CARTACEA

La gestione degli archi cartacei è demandata alle singole strutture le quali provvederanno alla sistemazione, manutenzione e controllo degli stessi nei limiti delle posiibilità e delle strutture.

FORMAZIONE / INFORMAZIONE

In questi ultimi anni sono stati approntati dei piani di sensibilizzazione inerenti la sicurezza della gestione dei dati sensibili in modo da affrontare, per ogni situazione specifica, le particolari problematiche. Il piano di formazione impostato è stato progettato con l'obiettivo di informare i responsabili e gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

A tale fine, il piano è stato suddiviso sulla base delle specifiche esigenze di ciascuna area aziendale in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati e sui criteri e modalità di evitare tali rischi.

I contenuti esposti sono:

- Informazioni sul D. Lgs. 196/2003, e sui principi legislativi comunitari.
- Funzionamento della normativa nell'ambito dei diritti del cittadino e comportamenti aziendali.
- Rischi possibili e probabili cui sono sottoposti i dati (con richiami a casi di crimini informatici, frodi, abusi, danni).
- Misure di sicurezza tecniche, organizzative e comportamentali deputate alla prevenzione dei rischi.
- Comportamenti e modalità di lavoro per prevenire i rischi.

Informativa capillare

Come precedentemente accennato, tutti i dipendenti della AUSL sono formalmente incaricati dei trattamenti di dati personali e sensibili nei rispettivi ambiti di trattamento.

Per questo motivo si è deciso di attuare una politica capillare d'informazione sui temi delCodice Privacy (D.Lgs. 196/03) e sui comportamenti necessari a tutelare il diritto del cittadino alla privacy.
E' in via di valutazione la modalità da adottare per comunicare capillarmente a tutti i dipendenti e collaboratori detta informativa.

Pubblicazione sulla intranet

Sulla intranet aziendale sarà pubblicata un'informativa generale riguardante gli obiettivi e i contenuti del D.Lgs. 196/2003.

A.V.E.N.

Un alto livello di integrazione tra le diverse componenti del Sistema Sanitario Regionale si rende necessario per garantire la pratica attuazione dei principi dell'universalismo, dell'inclusività e dell'equità di accesso ai servizi da parte del cittadino, in una organizzazione che storicamente tende fisiologicamente a privilegiare le dinamiche interne.
Già il Piano Sanitario della Regione Emilia-Romagna per il periodo 1999-2001 aveva provveduto a delineare l'assetto organizzativo-funzionale per la realizzazione dell'integrazione tra i servizi delle aziende. Successivamente è risultata evidente la necessità di allargare l'approccio all'ambito inter-aziendale al fine di realizzare ulteriori traguardi in termini di qualità dei servizi e livelli di efficienza.
Sulla base di medesimi principi la Regione Emilia Romagna ha adottato provvedimenti legislativi per la formazione e lo sviluppo di funzioni integrate sull'intero ambito regionale, ritenute strategiche ai fini della qualità dei servizi ai cittadini ed economicità della gestione.
Da queste considerazioni è stato redatto un documento che vuole essere una linea guida comportamentale, da affiancarsi e non sostituirsi a quello che costituisce l'allegato B della 196, scaturita dalla diretta esperienza delle singole aziende presenti in AVEN.

ELENCO ALLEGATI

- Allegato 01: P0701 Regole di gestione/conservazione delle credenziali di autenticazione;
- Allegato 02: P0702 Etica e norme di buon uso dei servizi di rete Internet;
- Allegato 03: P0700 Nomenclatura documenti;
- Allegato 04: T0201 Analisi dei rischi per apparecchiature Server;
- Allegato 05: T0202 Analisi dei rischi per Workstation;
- Allegato 06: T0203 Analisi dei rischi per apparecchiature di rete;
- Allegato 07: T0204 Analisi dei rischi per le applicazioni;
- Allegato 08: T0205 Misure di sicurezza;
- Allegato 09: T0301 Linee trasmissione dati ;
- Allegato 10: T0302 Elenco Strutture aziendali ;
- Allegato 11: P0101 Elenco Responsabili dei Trattamenti;
- Allegato 12: P0102 Elenco Responsabili Esterni;
- Allegato 13: T0303 Elenco Trattamenti dei dati;
- Allegato 14: P0703 Regolamento per l'utilizzo degli strumenti informatici dell'AUSL di Parma.
- Allegato 15: T0304 Elenco Server Aziendali;
- Allegato 16: P0103 Regolamento AVEN;
- Allegato 17: T0305 Elenco Connessioni VPN;
- Allegato 18: P0104 Videosorveglianza;

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0701

Oggetto : Regole di gestione/conservazione delle credenziali di autenticazione

Data Ultima Modifica :24/03/2010

La definizione e la gestione dell'account di autenticazione da parte di un utente ad un trattamento dati sono caratterizzate dalle seguenti regole comportamentali, che lo rendono responsabile di qualsiasi operazione di violazione e/o danneggiamento riconducibili a tali credenziali di accesso ai dati:

- La lunghezza minima della password è di 8 caratteri;
- La password deve contenere almeno un carattere alfabetico ed uno numerico;
- La password non deve contenere più di due caratteri identici consecutivi;
- La password non deve essere simile alla password precedente;
- La password non deve contenere il nome dell'utente o user-id;
- La password deve essere cambiata almeno ogni 3 mesi;
- La password non deve essere comunicata ad altri utenti.

Laddove la tecnologia lo permette, tali regole sono rese obbligatorie dal software applicativo, altrimenti è responsabilità dell'utente stesso applicarle e rispettarle.

Alcuni suggerimenti utili, per creare una password efficace, sono che la password deve essere facile da ricordare e presentare al tempo stesso difficoltà alle terze parti, che cercano di individuarla. Questo significa, che è preferibile scegliere una password, che **NON** sia riconducibile alla denominazione della propria attività piuttosto che a il numero di targa della propria auto o il nome di un proprio familiare.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0702

Oggetto : Etica e norme di buon uso dei servizi di rete Internet

Data Ultima Modifica :04/03/2008

Fra gli utenti dei servizi telematici di rete, prima fra tutte la rete Internet, si sono sviluppati nel corso del tempo una serie di "tradizioni" e di "principi di buon comportamento" (galateo) che vanno collettivamente sotto il nome di "netiquette". Tenendo ben a mente che la entità che fornisce l'accesso ai servizi di rete (provider, istituzione pubblica, datore di lavoro, etc.) può regolamentare in modo ancora più preciso i doveri dei propri utente, riportiamo in questo documento un breve sunto dei principi fondamentali della "netiquette", a cui tutti sono tenuti ad adeguarsi.

- Se si manda un messaggio, è bene che esso sia sintetico e descriva in modo chiaro e diretto il problema. Specificare sempre, in modo breve e significativo, l'oggetto (campo "Subject") del testo incluso nella mail. Se si utilizza un "signature file", mantenerlo breve e significativo;
- Se si risponde ad un messaggio, evidenziare i passaggi rilevanti del messaggio originario, allo scopo di facilitare la comprensione da parte di coloro che non lo hanno letto, ma non riportare mai sistematicamente l'intero messaggio originale, se non quando sia necessario;
- Non pubblicare mai, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica;
- Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano state sollecitate in modo esplicito;
- Non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività.

Alle regole precedenti, vanno aggiunti altri criteri che derivano direttamente dal buon senso:

- Qualunque attività che appesantisca il traffico o i servizi sulla rete, quali per esempio il trasferimento di archivi voluminosi o l'invio di messaggi di posta elettronica contenenti grossi allegati ad un gran numero di destinatari, deteriora il rendimento complessivo della rete. Si raccomanda pertanto di effettuare queste operazioni in modo da ridurre il più possibile l'impatto sulla rete. In particolare si raccomanda di:
  1. Effettuare i trasferimenti di archivi in orari diversi da quelli di massima operatività (per esempio di notte), tenendo presenti le eventuali differenze di fuso orario;
  2. Non inviare per posta elettronica grosse moli di dati; indicare (ove possibile) la locazione (URL) dei dati nel messaggio, rendendoli disponibili per il prelievo o la consultazione sulla rete.

- Il software reperibile sulla rete può essere coperto da brevetti e/o vincoli di utilizzo di varia natura. Leggere sempre attentamente la documentazione di accompagnamento prima di utilizzarlo, modificarlo o ridistribuirlo in qualunque modo e sotto qualunque forma;
- Comportamenti palesemente scorretti da parte di un utente, quali:
  1. Violare la sicurezza di archivi e computers della rete;
  2. Violare la privacy di altri utenti della rete, leggendo o intercettando la posta elettronica loro destinata;
  3. Compromettere il funzionamento della rete e degli apparecchi che la costituiscono con programmi (virus, trojan horses, ecc.) costruiti appositamente costituisce dei veri e propri crimini elettronici

e come tali sono punibili dalla legge.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0700

Oggetto : Nomenclatura documenti

Data Ultima Modifica:20/03/2007

Si definisce di seguito il sistema di numerazione delle procedure riguardanti il sistema di sicurezza e la documentazione del DPS in generale. Ogni documento sarà numerato secondo il seguente schema:

N YXX

Dove il significato delle lettere è il seguente....

Simbolo	***Valore***	***Significato***
N	P	Documento di procedura o definizione
	S	Schema, Diagramma o Flow Chart
	T	Tabella

Simbolo	***Valore***	***Significato***
Y	0	Sistema di sicurezza
	1	Identificazione e suddivisione delle funzioni e delle responsabilità.
	2	Analisi ed abbattimento del rischio
	3	Catalogazione delle fonti di dati e dei computers
	4	Configurazione e gestione degli apparati di rete, dei computers, sistemi operativi, applicativi. Procedura di aggiornamento o informativa.
	5	Autentificazione Utenti
	6	Integrità dei dati e disponibilità deis sistemi (backup, disaster recovery, gruppi di continuità)
	7	Formazione del personale

Simbolo	***Valore***	***Significato***
XX	XX	Progressivo all'interno dell'area tematica

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0201

Oggetto : Analisi dei rischi per apparecchiature Server

Data Ultima Modifica :19/03/2009

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le apparecchiature server.

Interruzione di Servizi

Evento	*I.R.*
Assenza di alimentazione	4
Manomissione volontaria	2
Accesso non autorizzato alla rete	5
Presenza di virus	5
Guasti Hardware	4
Errori umani non volontari	3
Uso improprio di autorizzazione di accesso	3
Sottrazioni autorizzazioni di accesso	1

f. Manomissioni archivi

Evento	*I.R.*
Incuria nella gestione	2
Comportamenti sleali o fraudolenti	1
Accesso non autorizzato alla rete	4
Guasti ai supporti di memorizzazione	3
Sottrazioni autorizzazione di accesso	1
Presenza Virus	3

o. **Intercettazione e diffusione dati**

Evento	*I.R.*
Accesso non autorizzato alla rete	4
Uso improprio di autorizzazione di accesso	4
Uso improprio dei dati	2

Evento	*I.R.*
Sottrazioni autorizzazione di accesso	3
Comportamenti sleali o fraudolenti	3
Presenza di Virus	3

Glossario:

I.R. : Indice di rischio

Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0202

Oggetto : Analisi dei rischi per Workstation

Data Ultima Modifica :19/03/2009

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le apparecchiature workstations.

Interruzione di Servizi

Evento	*I.R.*
Assenza di alimentazione	3
Manomissione volontaria	4
Accesso non autorizzato alla rete	5
Presenza di virus	5
Guasti Hardware	4
Errori umani non volontari	4
Uso improprio di autorizzazione di accesso	5
Sottrazioni autorizzazioni di accesso	6

g. Manomissioni archivi

Evento	*I.R.*
Incuria nella gestione	4
Comportamenti sleali o fraudolenti	3
Accesso non autorizzato alla rete	5
Guasti ai supporti di memorizzazione	2
Sottrazioni autorizzazione di accesso	6
Presenza Virus	5

p. **Intercettazione e diffusione dati**

Evento	*I.R.*
Accesso non autorizzato alla rete	5
Uso improprio di autorizzazione di accesso	5
Uso improprio dei dati	1

Evento	*I.R.*
Sottrazioni autorizzazione di accesso	5
Comportamenti sleali o fraudolenti	2
Presenza di Virus	4

Glossario:

I.R. : Indice di rischio

Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

Nome Documento : T0203

Oggetto : Analisi dei rischi per apparecchiature di rete

Data Ultima Modifica :19/03/2009

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le apparecchiature di rete.

Interruzione di Servizi

Evento	***I.R.***
Assenza di alimentazione	3
Manomissione volontaria	2
Accesso non autorizzato alla rete	3
Presenza di virus	1
Guasti Hardware	2
Errori umani non volontari	3
Uso improprio di autorizzazione di accesso	3
Sottrazioni autorizzazioni di accesso	3

h. **Intercettazione e diffusione dati**

Evento	***I.R.***
Accesso non autorizzato alla rete	3
Uso improprio di autorizzazione di accesso	2
Sottrazioni autorizzazione di accesso	2
Comportamenti sleali o fraudolenti	4

Glossario:

I.R. : Indice di rischio

Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0204

Oggetto : Analisi dei rischi per le applicazioni

Data Ultima Modifica :19/03/2009

Vengono di seguito riportate le principali categorie di rischio a cui sono soggette le applicazioni.

Manomissioni archivi

Evento	***I.R.***
Incuria nella gestione	3
Comportamenti sleali o fraudolenti	3
Accesso non autorizzato alla rete	5
Guasti ai supporti di memorizzazione	2
Sottrazioni autorizzazione di accesso	5
Presenza Virus	4

i. **Intercettazione e diffusione dati**

Evento	***I.R.***
Accesso non autorizzato alla rete	4
Uso improprio di autorizzazione di accesso	5
Uso improprio dei dati	4
Sottrazioni autorizzazione di accesso	5
Comportamenti sleali o fraudolenti	3
Presenza di Virus	4

Glossario:

I.R. : Indice di rischio

Rappresentato con una scala da 1 a 10 (10 = massimo valore) indica la possibilità che un evento si verifichi.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0205

Oggetto : Misure di sicurezza

Data Ultima Modifica :20/03/2009

Misure	Descrizione dei rischi contrastati	Trattamenti interessati	Misure già in essere	Misure da adottare	Struttura o persone addette all'adozione
Stock in magazzino di parti di ricambio specifiche	Deterioramento periferiche Input/Output	Tutti	Stato Effettivo	Controllo forniture di ricambio	Servizio RIT
Presenza UPS	Assenza alimentazione di rete	Tutti	Stato Effettivo	Monitoraggio del corretto funzionamento delle apparecchiature	Servizio RIT
Stock in magazzino di parti di ricambio specifiche	Rottura schede interne	Tutti	Stato Effettivo	Controllo forniture di ricambio	Servizio RIT
Installazione di software antivirus, protezioni hardware associate, politiche di gestione utenti.	Infezione delle macchine da attacchi malaware	Tutti	Stato Effettivo	Controllo forniture di nuovi aggiornamenti	Servizio RIT
Installazione di software antivirus, protezioni hardware associate, politiche di gestione utenti.	Infezione delle macchine da attacchi spam	Tutti	Stato Effettivo	Monitoraggio del corretto funzionamento delle apparecchiature	Servizio RIT

Accessi alle attrezzature controllate	Furto	Tutti	In fase di miglioramento	Incremento delle procedure di prevenzione	Servizio RIT
Istruzioni e formazione al personale	Uso improprio di credenziali	Tutti	Stato Effettivo – dopo aver effettuato corsi.	Aggiornamenti e corsi	Servizio RIT
Monitoraggio e apparecchiature di scorta	Mancanza di collegamenti di rete	Tutti	Stato Effettivo	Aggiornamento del personale e controllo magazzino	Servizio RIT
Messa in sicurezza della stanza dove risiedono le apparecchiature	Danni provocati da eventi accidentali	Tutti	In fase di miglioramento	Controlli di consistenza apparati di sicurezza	Servizio RIT
Operazioni Backup	Perdita dati accidentale e dolosa	Tutti	Stato Effettivo	Controlli di consistenza apparati di sicurezza	Servizio RIT

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0301

Oggetto : Linee di trasmissione dati

Data Ultima Modifica :23/04/2013

Di seguito le linee di trasmissione dati per la connettività delle sedi aziendali

0521 13048231	Ambulatorio Foschini Carla Via Unicef 11 - Monticelli Terme
0521 13053846	Avoprorit Traversetolo Piazza Fanfulla 45/B
0525 733017	Bardi Via Arandora Star 11
0525 13340677	Bardi Via Arandora Star 11
0525 13340610	Bedonia Piazza Caduti 1
0525 13340615	Borgotaro Distretto / Ospedale Via dei Benefattori 12
0525 13340604	Borgotaro Distretto / Ospedale Via dei Benefattori 12
0525 13340803	Borgotaro Veterinari Via Giuseppe Micheli 2
0524 13347147	Busseto Via Nicolò Paganini 13
0525 52243	Casa Protetta Calestano Via Del Bocco 1
0521 845023	Casa Protetta Cà Bonaparte Località Cà Bonaparte
0521 13046741	Casa Protetta Residenza Al Parco Via Bassi 4 - Monticelli
0521 896619	Casa Protetta Valcedra NEW Località Monchio Basso 11
0521 13704766	Casa Protetta Villa Benedetta Via Roma, 4
0525 13341114	Casa della salute di Berceto Salita Pietro Silva n° 7
0521 13046740	Casa di Cura Valparma Via XX Settembre 22
0521 13703993	Casa di Padre Lino ONLUS Viale Caprera 16
0521 13053889	Centro Autismo Via La Spezia 142
0524 13347016	Centro Casa il Ponte Via Piave 19/A
0524 13347151	Centro Disturbi Cognitivi Via Tincati 2
0525 13340611	Centro Medico Borgotaro Via Bellinzona 2
0521 849002	Centro Prel. Scurano c/o Ambulatorio Croce Rossa Località Mercato 1 - Scurano
0521 894030	Centro Prelievi Palanzano Strada del Torchio 3
0521 869002	Centro Prelievo Tizzano Via Europa Unita 41
0521 13048658	Centro Salute Mentale - Gruppo Appartamento Via Po 72
0521 13053863	Collecchio Via Berlinguer 2
0521 13046721	Collecchio Veterinari Via Spezia 89
0521 13046698	Colorno - Polo Sanitario Via Suor Maria, 1
0521 13046775	Colorno - Polo Sanitario Via Suor Maria, 1
0521 13004706	Colorno I Maggio Via Roma 16
0521 849021	Comune Neviano degli Arduini P.zza IV Novembre 1
0521 13054096	Corniglio Piazza Castello 1/3
0521 13046406	Dialisi Sala Baganza Strada del Mulino
0521 13046742	Don Gnocchi Piazzale dei Servi 3
0521 13048975	Drop In Strada dei Mercati 9/B
0521 13048657	Fattoria di Vigheffio Via Vigheffio 17
0521 13048232	Felino Via Perlasca
0524 13347144	Fidenza Casa Protetta Berenini Via Berenini 151
0524 13347145	Fidenza Casa Protetta Berenini Via Berenini 151
0524 13346988	Fidenza Ospedale Vaio Località Cabriolo
0524 530197	Fidenza Ospedale Vaio Località Cabriolo
0521 13047985	Fontanellato Casa Riposo Via XXIV Maggio
0525 13340616	Fornovo - Polo Territoriale Via Solferino 52
0525 13340606	Fornovo - Polo Territoriale Via Solferino 52

0521 13703985	Gruppo Galeno Via Musini 2/b
0521 13700029	Gruppo Pablo Via La Grola 5
0521 13703995	Gruppo San Moderanno Via Trieste 108
0521 13046778	Langhirano Distretto Via Roma 42/1
0521 13046694	Langhirano Distretto Via Roma 42/1
0525 422177	Medesano Poliambulatorio Piazza Rastelli
0525 13340721	Medesano Poliambulatorio Piazza Rastelli
0521 13053853	Noceto Via Gen C.A. Dalla Chiesa 30
0521 13004870	Padiglione Braga c/o Azienda Ospedaliera
0521 13045165	Parma - Carcere Via Burla 56
0521 13346375	Parma - Sert Via del Taglio Via del Taglio 2
0521 13046681	Parma - Ugolino Strada del Quartiere 2/A
289765392	Parma - Ugolino Strada del Quartiere 2/A
344733020	Parma - Ugolino Strada del Quartiere 2/A
0521 13046679	Parma - Ugolino Strada del Quartiere 2/A
800 354276	Parma - Ugolino Strada del Quartiere 2/A
800 255671	Parma - Ugolino Strada del Quartiere 2/A
0521 383722	Parma - Ugolino Strada del Quartiere 2/A
0521 383721	Parma - Ugolino Strada del Quartiere 2/A
0521 13347047	Parma - Ugolino Strada del Quartiere 2/A
0521 13345245	Parma - Ugolino Strada del Quartiere 2/A
0525 13340061	Parma - Ugolino Strada del Quartiere 2/A
0521 13046726	Parma - Via Carmignani Via Carmignani 13
0521 13046714	Parma Cup Lubiana Parma Est Via Leonardo Da Vinci 43
0521 13046773	Parma Cup Via Pintor Via Pintor 1
0521 13046700	Parma Cup Via Pintor Via Pintor 1
0521 13053861	Parma Cup Via Verona Via Verona
0521 13053854	Parma Cup Via Verona Via Verona
0521 13046716	Parma Distretto Viale Basetti 8
0521 13048397	Parma Magazzino Via Franklin 31
0521 13048656	Parma Medicina Dello Sport Via Silvio Pellico 14/A
0521 944212	Parma Rasori Viale Gramsci 14
0521 13040029	Parma Sert Strada dei mercati 15/B
0521 13346899	Parma Sert Strada dei mercati 15/B
0521 13048976	Parma Ugolino Router strada del quartiere 2/a
0521 13048977	Parma Ugolino Router strada del quartiere 2/a
0521 13048800	Parma Via Savani Via Savani - Via I. Bocchi 31
0521 13046729	Parma Via Turchi Via Turchi 5
0521 13048403	Parma Via Vasari Via Vasari
0521 13048408	Parma Via Vasari Via Vasari
0521 13046732	Parma Via XXII Luglio Via XXII Luglio
0521 13046735	Parma Via del Campo Via Giuseppe del Campo 12
0521 247668	Parma Via del Campo Via Giuseppe del Campo 12
0524 594928	Pellegrino Veterinari Via Roma 8/B
0525 60430	Poliambulatorio Berceto Piazza Micheli 5
0521 3046722	Programma Adolescenza Via Mazzini 2

0521 13704292	Residenza Villa Matilde Via Bracchi 10
0524 13347146	Salsomaggiore Parco G. Mazzini 11
0521 13046727	San Polo di Torrile Via M.Margotti 2
0521 13046776	San Secondo Via V. Mazza 1
0521 13046696	San Secondo Via V. Mazza 1
0521 13048233	Servizio Attivita Tecniche Via Spalato 2
0524 13347224	Servizio Sociale Parco Mazzini 4
0521 13046728	Sorbolo Via al Donatore 2
0521 13053887	Sorbolo Avis Via Gruppini 4/Bis
0521 13345407	Spazio Giovani Via Melloni 1/B
0521 13046723	Spazio Giovani Via Melloni 1/B
0521 687100	Tortiano Strada S. Solari
0521 13048411	Traversetolo DUC Via IV Novembre 33
0521 13048404	Traversetolo DUC Via IV Novembre 33
IDSDH 1-4-5 / 6	Ugolino Internet Strada del Quartiere 2/A

Sono inoltre installati tre PAL di Lepida nelle sedi di Parma Ugolino, Fidenza Vaio e Ospedale di Borgo val di Taro

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0302

Oggetto : Elenco Strutture Aziendali

Data Ultima Modifica :23/04/2013

STRUTTURA	INDIRIZZO
Sede Centrale "Ex ospedale Ugolino da Neviano"	Strada del Quartiere n°2/a
Dipartimento per la qualità e l'accreditamento	Via Spalato n°4
Servizio Attività Tecniche e Servizio Economato	Via Spalato n°2
Servizio Prevenzione e Protezione Aziendale	Via Spalato n°4
Magazzino Economale	Via Franklin n°31 c/o Centro Ingrosso "La Cittadella"
Servizio Farmaceutico	c/o Azienda Ospedaliera
Chiesa S. Maria del Quartiere	Strada del Quartiere
Punto Bianco	c/o Azienda Ospedaliera - Padiglione Monoblocco

Appartamenti Psichiatrici (n°8 alloggi)	Via Corso Corsi n°54
Appartamenti psichiatrici protetti ("Ex Scoiattolo")	Via Mamiani della Rovere n°5
Appartamento per disabili	Via Pasubio n°42
Appartamento Psichiatrico	Viale Piacenza n°72
Appartamento Psichiatrico	Via Olivieri n°11
Appartamento Psichiatrico	Borgo Guazzo n°22
Appartamento Psichiatrico	Via Passo delle Guadine n°9
Appartamento Psichiatrico	Via Cocconi n°15
Appartamento Psichiatrico	Via Po n°42
Appartamento Psichiatrico	Via Taro n°25
Appartamento Psichiatrico	Via Aleotti n°13
Appartamento Psichiatrico	Via Aleotti n°26
Appartamento Psichiatrico	Via Lucrezio Caro n°10
Appartamento Psichiatrico	Viale Vittoria n°31
Appartamento Psichiatrico	Via Costituente n°8
Appartamento Psichiatrico	Via Pasubio n°30
Appartamento Psichiatrico	Via Pasubio n°33
Appartamento Psichiatrico	Via Pasubio n°58
Appartamento Psichiatrico	Via Marchesi n°29
Appartamento Psichiatrico	Via Goito n°3
Appartamento Psichiatrico	Via Savani n°11
Appartamento Psichiatrico	Via Budellungo n°16
Appartamento Psichiatrico	Via Bianchi n°5

Appartamento Psichiatrico	Via Jacchia n°19
Appartamento Psichiatrico	Via Catullo n°18
Gruppo appartamento disabili	Via Passo delle Guadine n°3
Centro Autismo	Loc. Marinelli - Via La Spezia n°147
Centro Disabili Gravi "Lubiana"	Via Oradour n°16
Centro Disabili Gravi "Varese"	Via Varese n°9
Centro Diurno Disabili Gravi "Raimondi"	Via Casaburi c/o ASP "Ad personam"
Centro Diurno Psichiatrico "Il Filo d'Arianna"	Via Po n°70/72
Centro Senologico "Bagnasco"	c/o Azienda Ospedaliera - Padiglione Monoblocco
Centro Salute Mentale Parma Est	Via Turchi n°5/a
Centro Polifunzionale Ex Osp.Civile S. Mauro Abate	Via Suor Maria n°3 - COLORNO
Centro Psichiatrico "Santi" - Associazioni del volontariato	Via Reggio n°43
Centro Psichiatrico "Santi" - Centro Salute Mentale Parma Ovest	Via Reggio n°43
Centro Psichiatrico "Santi" - Day Hospital Psichiatrico	Via Reggio n°43
Centro Psichiatrico "Santi" - Residenza	Via Reggio n°43
Consultorio Demenze	Via Del Campo
Diagnosi e Cura	c/o Padiglione "Braga" AO
Dipartimento di Sanità Pubblica	Via Vasari n°13/a
DUS	L.go Palli 11/a
Medicina dello Sport	Via Pellico n°14 c/o Palazzetto dell Sport
Neuropsichiatria Infantile	Via Bocchi n°1/a
Pediatria di comunità - Laboratorio informatico	Via Vasari n°13/a
Polo Sanitario "Vilma Preti"	Via Verona n°23/a
Polo Sanitario Parma Centro	Viale Basetti n°8
Polo Sanitario Parma Est	Via Leonardo da Vinci n°42
Polo Sanitario Parma Ovest	Via Pintor n°1
Polo Sanitario Parma Sud	Via Carmignani n°13/a
Polo Sanitario di Sorbolo	Via dei Donatori n°2 - SORBOLO
Programma adolescenza e Disturbi alimentari	Via Mazzini n°2
Punto prelievi di Sorbolo	Via Gruppini n°4/bis - SORBOLO
Residenza Psichiatrica "I° Maggio"	Via Roma n°16 - COLORNO
Residenza Psichiatrica di Casale di Mezzani	Via IV Novembre n°4 - MEZZANI
Residenza Psichiatrica di Torrile	Via Margotti - S.POLO DI TORRILE
SER.T.	Strada dei Mercati n°15/b
SER.T. Centro Distribuzione Metadone	Via del Taglio

SER.T. Drop-In	Strada dei Mercati
Spazio Giovani	Via Melloni
Spazio Salute Immigrati	Via XXII Luglio n°27

Centro Prelievi-Ufficio Igiene c/o ex Gesuiti	Via Berenini n°151 - FIDENZA
Centro Residenziale per Disabili "Il Ponte"	Via Piave n°19/a - FIDENZA
CUP c/o ex Gesuiti	Via Berenini n°151 - FIDENZA
Laboratorio educativo di Fidenza	Via Marchetti n°2 - FIDENZA
Poliambulatori di Busseto	Via Paganini n°13 - BUSSETO
Poliambulatori di Fontanellato	Via XXIV Maggio n°16/a - FONTANELLATO
Poliambulatori di Noceto	Via Dalla Chiesa n°30 - NOCETO
Poliambulatori di Salsomaggiore	Via Roma n°9/a - SALSOMAGGIORE
Poliambulatori di San Secondo (Corpo B)	P.zza Martiri della Libertà - SAN SECONDO
SER.T. c/o ex-Gesuiti	Via Berenini n°153 - FIDENZA
SIMAP di Fidenza c/o ex-Gesuiti	Via Berenini n°153 - FIDENZA
Sistema di Accoglienza di Vaio	Via Don Enrico Tincati n°5 - loc. Vaio - FIDENZA

Ambulatori di Calestano	Via Bocco n°1 - CALESTANO
Ambulatori di Corniglio	Via Castello n°1/3 - CORNIGLIO
Ambulatori di Felino	Via Perlasca n°9 - FELINO
Ambulatori di Monchio delle Corti	Via Monchio Basso n°1 - MONCHIO DELLE CORTI
Ambulatori di Neviano degli Arduini	Via IV Novembre n°3 - NEVIANO DEGLI ARDUINI
Ambulatori di Palanzano	P.zza Ferrari - PALANZANO
Ambulatori di Sala Baganza	Piazza Garibaldi n°1 - SALA BAGANZA
Ambulatori di Tizzano	Via della Croce Rossa n°3 - TIZZANO
Appartamento Psichiatrico	Via Banzola n°18 - LANGHIRANO
Appartamento Psichiatrico	Via Banzola n°16 - LANGHIRANO
Centro Dialisi di Sala Baganza	Via del Mulino - SALA BAGANZA
Complesso Psichiatrico "La Fattoria" - Appartamenti	Strada Vigheffio n°17 - COLLECCHIO
Complesso Psichiatrico "La Fattoria" - Archivio	Strada Vigheffio n°17 - COLLECCHIO
Complesso Psichiatrico "La Fattoria" - Residenza	Strada Vigheffio n°17 - COLLECCHIO
Polo Sanitario di Monticelli	Via Bassi - MONTICELLI
Poliambulatori "Il Duca" di Traversetolo	Via IV Novembre n°35 - TRAVERSETOLO
Centro Socio Sanitario di Collecchio	Via Berlinguer n°2 - COLLECCHIO

Polo Socio Sanitario di Langhirano - Poliambulatori	Via Roma n°42/1- LANGHIRANO
Polo Socio Sanitario di Langhirano - Centro Cure Progressive	Via Allende n°2 - LANGHIRANO
Servizio Veterinario di Collecchio	Via Spezia n°89/b - COLLECCHIO

Ambulatori di Bardi	Via Arandora Star n°11 - BARDI
Ambulatori di Bedonia	P.zza Caduti per la Patria n°1 - BEDONIA
Ambulatori di Berceto	P.le Micheli n°4 - BERCETO
Archivi di Pontolo	Loc. Pontolo - BORGOTARO
Polo Odontoiatrico di Medesano	Piazza Rastelli n°3 - MEDESANO
Polo Sanitario di Fornovo Taro ex aeronautica	Via Solferino n°37 - FORNOVO TARO
Polo Sanitario di Medesano	Piazza Rastelli n°1 - MEDESANO
Servizio Veterinario (ex Igiene Pubblica)	Via Micheli n°2 - BORGOTARO

Ospedale "Santa Maria" di Borgotaro	Via Benefattori n°12 - BORGOTARO
Ospedale di San Secondo Parmense (Corpo A)	Via M. Vitali Mazza n°3 - SAN SECONDO
Ospedale di Vaio	Via Don Enrico Tincati n°5 - loc. Vaio - FIDENZA

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0101

Oggetto : Elenco Responsabili dei Trattamenti

Data Ultima Modifica :23/04/2013

PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOLOGIA	GODIO	MARTA
PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOLOGIA	STEFANINI	SILVIA
PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOLOGIA	ABBIATI	SIMONA MARIA
PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOLOGIA	VENTIMIGLIA	ANNA
PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOTERAPIA	CABASSI	ANDREA
PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOTERAPIA	ZILIOLI	CLAUDIA
PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOTERAPIA	KUNTZE	CARLOTTA ROSSELLA
PARMA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NPIA Psicologia Clinica - Parma	DIR.PSICOLOGO-PSICOTERAPIA	BORGATTI	ELISABETTA
PARMA Distretto	DIPARTIMENTO CURE PRIMARIE	CONSULTORIO DEMENZE VIA SIDOLI	DIR.PSICOLOGO-PSICOLOGIA	COPELLI	SANDRA
PARMA Distretto	DIPARTIMENTO CURE PRIMARIE	CONSULTORIO DEMENZE VIA SIDOLI	DIR.PSICOLOGO-PSICOLOGIA	NUCERA	VALENTINA
PARMA Distretto	DIPARTIMENTO CURE PRIMARIE	CONSULTORIO DEMENZE VIA SIDOLI	DIR.PSICOLOGO-PSICOLOGIA	DIECI	FRANCESCA
PARMA Distretto	DIPARTIMENTO CURE PRIMARIE	SALUTE DONNA PARMA CENTRO	DIR.PSICOLOGO-PSICOTERAPIA	VITALI	VILLIAM
PARMA Distretto	DIPARTIMENTO CURE PRIMARIE	SALUTE DONNA: SPAZIO GIOVANI PARMA	DIR.PSICOLOGO-PSICOLOGIA	BRANCHI	BARBARA
FIDENZA Distretto	SERVIZI GENERALI	PERSONALE FIDENZA LUNGHE ASSENZE/NON IN SERVIZIO	DIR.AMMINISTR. - SENZA DISCIPLINA	ROSSI	GRAZIANA
FIDENZA Distretto	DIPARTIMENTO SANITA' PUBBLICA	PREV.SIC.AMB.LAV. FIDENZA DIRIG.	DIR. INGEGNERE	CASTELLOTTI	PIETRO
FIDENZA Distretto	DIPARTIMENTO SANITA' PUBBLICA	IG.ALIMENTI E NUTR.FIDENZA DIRIG.	DIR.CHIM. IGIENE ALIMENTI/NUTRIZ.	SAVI	FEDERICA
FIDENZA Distretto	DIPARTIMENTO FARMACEUTICO	FARMACIA AZIENDALE DIRIGENTI	DIR.FAR. FARMACIA OSPEDALIERA-DIRETTORE	GAZZOLA	ANNA MARIA
FIDENZA Distretto	DIPARTIMENTO FARMACEUTICO	FARMACIA AZIENDALE DIRIGENTI	DIR.FAR. FARMACIA OSPEDALIERA	BORGHESI	SILVIA
FIDENZA Distretto	DIPARTIMENTO FARMACEUTICO	FARMACIA AZIENDALE DIRIGENTI	DIR.FAR. FARMACIA OSPEDALIERA	SANTORO	MATTEO
FIDENZA Distretto	DIPARTIMENTO FARMACEUTICO	FARMACIA AZIENDALE DIRIGENTI	DIR.FAR. FARMACIA OSPEDALIERA	ZOPPI	SILVIA
FIDENZA Distretto	DIPARTIMENTO FARMACEUTICO	FARMACIA AZIENDALE DIRIGENTI	DIR.FAR. FARMACIA OSPEDALIERA	MANFERDINI	MONICA
FIDENZA Distretto	DIPARTIMENTO FARMACEUTICO	FARMACIA AZIENDALE DIRIGENTI	DIR.FAR. FARMACIA OSPEDALIERA	SPINICELLI	SILVIA
FIDENZA Distretto	DIPARTIMENTO FARMACEUTICO	FARMACIA AZIENDALE DIRIGENTI	DIR.FAR. FARMACIA OSPEDALIERA	SANTI	PRIMO

FIDENZA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	SERT FIDENZA DIRIGENTI	DIR.PSICOLOGO-PSICOLOGIA	BARATTA	ANNA MARIA
FIDENZA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NEUROPSICH. INF.FIDEN DIRIGENTI	DIR.PSICOLOGO-PSICOLOGIA	PATTINI	MARIANNA
FIDENZA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NEUROPSICH. INF.FIDEN DIRIGENTI	DIR.PSICOLOGO-PSICOLOGIA	LEONI	LORENA
FIDENZA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NEUROPSICH. INF.FIDEN DIRIGENTI	DIR.PSICOLOGO-PSICOTERAPIA	PIGATI	SIMONETTA
FIDENZA Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NEUROPSICH. INF. S.SECONDO DIRIG.	DIR.PSICOLOGO-PSICOTERAPIA	ROSANI	SILVANO
FIDENZA Distretto	DIPARTIMENTO CURE PRIMARIE	SAL.DONNA S.SECONDO DIRIGENTI	DIR.PSICOLOGO-PSICOTERAPIA	AMBROGI	ANNA
FIDENZA Distretto	DIPARTIMENTO CURE PRIMARIE	NUCLEO CURE PRIMARIE FIDENZA DIRIG.	DIR.PSICOLOGO-PSICOLOGIA	CASANA	ELISA
FIDENZA Presidio Ospedaliero	SERVIZI GENERALI	DIR. SANIT. OSP. FID. S.S. DIRIG.	DIR.AMMINISTR. - SENZA DISCIPLINA	CANTINI	MARIO
FIDENZA Presidio Ospedaliero	DIPARTIMENTO DI PATOLOGIA CLINICA	LABORATORIO ANALISI - FIDENZA DIRIG.	DIR.BIO. PATOLOGIA CLINICA	PREVITALI	GIUSEPPE
FIDENZA Presidio Ospedaliero	DIPARTIMENTO DI PATOLOGIA CLINICA	LABORATORIO ANALISI - FIDENZA DIRIG.	DIR.BIO. PATOLOGIA CLINICA	MALPELI	MONICA
FIDENZA Presidio Ospedaliero	DIPARTIMENTO DI PATOLOGIA CLINICA	LABORATORIO ANALISI - FIDENZA DIRIG.	DIR.BIO. PATOLOGIA CLINICA	UGOLOTTI	GIUSEPPE
FIDENZA Presidio Ospedaliero	DIPARTIMENTO DI PATOLOGIA CLINICA	LABORATORIO ANALISI - FIDENZA DIRIG.	DIR.BIO. PATOLOGIA CLINICA	MARADINI	FABIO
FIDENZA Presidio Ospedaliero	DIPARTIMENTO DI PATOLOGIA CLINICA	LABORATORIO ANALISI - FIDENZA DIRIG.	DIR.BIO. PATOLOGIA CLINICA	UGGERI	JACOPO
BORGOTARO Distretto	SERVIZI GENERALI	AMM. - UFFICI AMMINISTRATIVI BORGOTARO	DIR.AMMINISTR. - SENZA DISCIPLINA	FAZIO	MARIA
BORGOTARO Distretto	SERVIZI GENERALI	AMM. - UFFICI AMMINISTRATIVI BORGOTARO	DIR.AMMINISTR. - SENZA DISCIPLINA	BRUNETTI	TIZIANA
BORGOTARO Distretto	DIPARTIMENTO SANITA' PUBBLICA	DSP - SPSAL - BORGOTARO	DIR. INGEGNERE	LOVISATTI	FRANCESCA
BORGOTARO Distretto	DIPARTIMENTO FARMACEUTICO	FARMACEUTICA BORGOTARO	DIR.FAR. FARMACEUTICA TERRIT.	PETRILLI	ANTONELLA
BORGOTARO Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	DAISMDP - PSICHIATRIA BORGOTARO	DIR.PSICOLOGO-PSICOLOGIA	BRUNI	BARBARA
BORGOTARO Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	DAISMDP - NEUROPSICHIATRIA INFANTILE BORGOTARO	DIR.PSICOLOGO-PSICOLOGIA	BERTOLI	SILVIA
BORGOTARO	DAI / SALUTE MENTALE	DAISMDP -	DIR.PSICOLOGO-PSICOLOGIA	GRAZIOLI	ALBERTO

Distretto	DIPENDENZE PATOLOGICHE	NEUROPSICHIATRIA INFANTILE FORNOVO			
BORGOTARO Distretto	DIPARTIMENTO CURE PRIMARIE	DCP - HOSPICE VALLI TARO E CENO	DIR.PSICOLOGO-PSICOLOGIA	LAVEZZI	MARIA
BORGOTARO Presidio Ospedaliero	DIPARTIMENTO DI PATOLOGIA CLINICA	LABORATORIO ANALISI - B.TARO	DIR.BIO. PATOLOGIA CLINICA	BERTONCINI	LUCA
BORGOTARO Presidio Ospedaliero	DIPARTIMENTO FARMACEUTICO	FARMACIA OSPEDALE B.TARO	DIR.FAR. FARMACIA OSPEDALIERA	BOFFETTI	MARILENA
BORGOTARO Presidio Ospedaliero	DIPARTIMENTO FARMACEUTICO	FARMACIA OSPEDALE B.TARO	DIR.FAR. FARMACIA OSPEDALIERA	CREMASCHI	FRANCESCA
SUD/EST Distretto	SERVIZI GENERALI	PERSONALE SUD-EST LUNGHE ASSENZE/NON IN SERVIZIO	DIR.PSICOLOGO-PSICOLOGIA	PALOMBI	FRANCESCA
SUD/EST Distretto	DIPARTIMENTO SANITA' PUBBLICA	SIAN SUD-EST	DIR.CHIM. IGIENE ALIMENTI/NUTRIZ.	REVERBERI	LUCIA
SUD/EST Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	SERT TERRITORIALE SUD-EST	DIR.PSICOLOGO-PSICOLOGIA	AZZALI	CRISTINA
SUD/EST Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NEUROPSICH. INF. LANGHIRANO	DIR.PSICOLOGO-PSICOLOGIA	MOI	GABRIELE
SUD/EST Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NEUROPSICH. INF. LANGHIRANO	DIR.PSICOLOGO-PSICOTERAPIA	ALZAPIEDI	ANAHI
SUD/EST Distretto	DAI / SALUTE MENTALE DIPENDENZE PATOLOGICHE	NEUROPSICH. INF. COLLECCHIO	DIR.PSICOLOGO-PSICOTERAPIA	MANETTA	DANIELA

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

ALLEGATO 12

Nome Documento : P0102

Oggetto : Elenco Responsabili Esterni

Data Ultima Modifica :23/04/2013

Farmacia Nazionale	Chiesi Dott. Anita	P.le V. Emanuele 19	Parma
Farmacia Guareschi	Farnetti Dr. Alberto	V. Farini 5/c	Parma
Farmacia Bordi Ozzano Taro	Bordi Dr.ssa Renata	v. Nazionale, 81	Ozzano Taro
Farmacia Comunale Collecchio	Raffi Dr.ssa Silvana	v. Togliatti, 6/a	Collecchio
Farmacia Mentana	Bonfanti Dott. Clara	V.le Mentana 1/e	Parma
Farmacia XXII Luglio s.n.	Lucchetti Dott. Natalia	V. XXII Luglio 13	Parma
Farmacia Landini	Landini Barbara	Via Emanuele 49	Sala baganza
Farmacia Montebello	Coperchini Dott. Bianca	V. Montebello 84/d	Parma
Poliamb. Dalla Rosa Prati	Melegari Elena	Via Emilia Ovest, 12/A	parma
Studio Medico Gallani	Gallani Roberto	l.go VIII Marzo, 11	Parma
INPAL	dott. Begani	v. Inzani, 23	Parma
Farmacia Tomatis	Tomatis Dott. Roberto	V. Toscana 94/a	Parma
Farmacia Parenti	Parenti Dr.ssa Micaela	V. D. Alighieri 2/a	Chiozzola
Farmacia Leporati	Eredi Dott. Leporati	V. Silvio Pellico 5/e	Parma
Farmacia Allegri	Maggiorelli dott.M.Cristina	V. Repubblica, 70/b	Parma
Farmacia Melegari	Melegari Dott. Pierangelo	V. P. Savani 1/a	Parma
Farmacia Santa Fara	Riccardi Dr.ssa Rosanna	v. Trieste 42/a	Parma
Farmacia Cordero	Merli Dott. Alessandro	str. Asolana 31	S.Polo di Torrile
CISL Parma	Pellegrini Silvia	V. Lanfranco	Parma
Asscom Parma	Carpi Luciano	Via Abbeveratoia 63/a	parma
CGIL Parma	Devincenzi, Pollari	V. Confalonieri, 151	Parma
Farmacia Bixio	Pattini Dott. Pier Luigi	str. Bixio, 5	Parma
Farmacia Coop. Gibertini	Manfredi Dott. Umberto	V. Repubblica 10/a	Parma
Farmacia Bottego	Chiesi Dott. Alberto	V.le Bottego 1/a	Parma
Farmacia Donetti Collecchio	Giovanelli Dr.ssa Maria Cristina	p. Avanzini, 1	Collecchio
Farmacia S. Lazzaro	Lusuardi Senatore Dr. Pietro	v. XXIV Maggio 10/a	Parma
Farmacia Cassitto	Cassitto Dr. Antonio	v. F. Parri 41/g	Parma
Farmacia S. Ilario	Ruggiero Dr.ssa Tina	p.le Lubiana 31/a	Parma
Farmacia Corradini	Corbellini Dott. Paola	V. Repubblica 20	Parma
Farmacia Ponte Dattaro	Bruschi Dr. Enrico	Str. Montanara, 23/b	Parma
Centro Fisioterapitco M.Luigia	Cavazzini lucia	Strada della Repubblica, 47	parma
Farmacia Landini	Landini Dott. Giovanni	V.le V. Emanuele 39	Sala Baganza
AVIS Vigatto (Corcagnano)	Colla Paolo-Benassi Adriano	v. donatori sangue 4	Corcagnano
Farmacia Baganza	Barbieri dott. Marco	V. Baganza 11/a	Parma
Farmacia comunale Mille	Molinari Dr. Mauro	V.le dei Mille, 52b	Parma
Farmacia Colajacomo	Colajacomo Dott. Adele	P.le Pablo 5/d	Parma
Farmacia SS. Annunziata	Barbieri Laura	via Gramsci 1/e	Parma
Farmacia Crocetta	Balderi Dott. Marco	V. Emilia Ovest	Parma
Farmacia Mantovani	Mazzocchi Dott. Alessandro	V. Garibaldi 281b	Parma
Farmacia comunale Fleming	Molinari Dr. Mauro	V. Fleming	Parma
Farmacia Pezzana	Gerevini Dr. Alberto	v. Bixio, 72	Parma
Farmacia Costa	Costa Dott. M. Grazia	Via Callani 20	Parma
Farmacia Cavallina	Pezzani Dr. Giulio	v. Emilio Lepido, 4/b	Parma

Farmacia San Biagio	Cimardi Raffaella	str. Allende 3	Torrile
Farmacia Romano	Rocco Gavazzoli	v. Solferino 34/c	Parma
Farmacia S.Filippo Neri	Fietta Dr.ssa Marina	v. Emilia Ovest, 151/b	S. Pancrazio - Parma
Farmacia Prati Bocchi	Turco dr. Paolo Cesare	v. Gramsci, 15/b	Parma
Farmacia Amadasi	Corbelli Dr.ssa Nella	v. S. Pertini, 10	Parma
Farmacia Fornari	Fornari Dr.ssa Beatrice	V. Farini 42/a	Parma
Farmacia S. Francesco	Del Porto Dr.ssa Giuseppina	V. Spezia 3/a	Parma
Farmacia Crocetta	Tegoni Dott. Paolo	V. Emilia Ovest	Parma
Farmacia comunale Campioni	Molinari Dr. Mauro	V. Campioni	Parma
Farmacia S. Leonardo	Cantarelli Dott. Tilde	V.Genova 2/a	Parma
Farmacia Stadio Tardini	Mezzadri Dr.Ursula e Sonia	P.le Risorgimento 11c	Parma
Farmacia S. Martino	Busani Dot.. Franco	V.Trento, 59a	Parma
Farmacia Siviero	Siviero Dott. Giampiero	V. Matteotti 16	Colorno
Farmacia Torri di Basilicanova	Laurenti Francesca	Via Argini Sud, 25	Basilicagoiano
Farmacia Venezia s.n.c.	Agnoletti Dott. Massimo	V. Valenti 3/e	Parma
Farmacia Volturno	Negri Dott. Maria	V. Volturno 761b	Parma
Farmacia Zanetti	Zanetti Dott. Filippo	Str. Vecchia di Bag. 51	Parma
Farmacia Zarotto	Chierici Dott. Nadia	V. Zarotto 30/e	Parma
Farmacia Silvia	Mossini dr.ssa Paola	v. Cavour, 23	Colorno
Farmacia Comunale Iezzi	Iezzi Dr.ssa Miriam	v. Roma, 34	Fontevivo
CISL Fidenza	Pellegrini Silvia	V. Mazzini, 26	Fidenza
Comune Polesine	Contini Maria Rosa	v.le delle Rimembranze, 12	Polesine
CGIL Fidenza	Colombini, Ghirardi	V. XX Setetmbre, 42	Fidenza
Farmacia San Donnino	Contini Dott.ssa Paola	l.go Leopardi, 2	Fidenza
Farmacia Malchiodi	Malchiodi dr. Paolo	P.za Garibaldi, 42	Fidenza
Farmacia Mainardi	Mainardi dott.ssa Katia	via Ghiara Sabbioni 15	Fontanellato
Farmacia Concari	Concari dott. Luiigino	v. Provinciale 39	Fontanelle
Comune Salsomaggiore	Gorra Lorena	p.zza Libertà, 1	Salsomaggiore Terme
UIL Salsomaggiore	Argentieri	V. Pascoli	Salsomaggiore
Farmacia Cuoghi	Cuoghi Dott. Iginio	via Tabiano, 63	Tabiano terme
Farmacia Parolari	Parizzi Dr.ssa Donatella	v. Berenini, 82	Fidenza
Farmacia S. Vitale	Franzan Dott. Giuseppe	V. Vaccari 17	Fontanellato
Comune Soragna	Melzi	P.le Meli Lupi, 1	Soragna
Farmacia Pelizza s.n c.	Arfini Dott. Lindo	P.za Garibaldi 26	Soragna
Farmacia Romanini	Romanini Dott. Carlo	V. Gramsci, 14	Noceto
Farmacia Zacconi	Bustaffa Dr. Stefano	v. Cavour, 21	Fidenza
Farmacia Gemignani	Gemignani Dr.ssa Elisabetta	v. Berenini, 26	Fidenza
Farmacia Fontevivo	Pasquali Alessandra	V. Roma, 36	43010
Comune Zibello	Michelazzi	V. Matteotti, 10	Zibello
Farmacia Cavalli	Pezzani Marina	v. Emilio Lepido, 4/b	43100
Farmacia Riccardi	Riccardi Dr. Andrea	V. Emilia 14/c	Ponte Taro
Farmacia Centrale	Lunardini Dott. Maria	P.zza Repubblica 23	Noceto
Farmacia Spotti	Spotti Dott. Patrizia	V. Statale 122	Castione Marchesi
Farmacia Raggi	Raggi Dott. Anna	P.za Micheli 28	Bedonia
Farmacia Rosso	Scamoni Dott. Isabella	V. Roma 26	Bore
Farmacia Scimonelli	Simoncelli Dr. Piergiuseppe	V. Roma 18	Varsi

Farmacia S. Giovanni	Dott.sse Rita e Donatella Surace	v. P. Cella 25	Bardi
Farmacia S. Rocco	Feccia Dott. Tiziana	V. Stazione 14	Valmozzola
Farmacia S. Giovanni	Virgilio Dott. Giuseppe	V. Colla 25	Bardi
Farmacia Denegri	Denegri Dott. Antonella	V. Puccini 2	S. Andrea Bagni
Farmacia S. Angela	Schianchi Dott. Eugenio	V. Principale	Albareto
Farmacia Corbelletta	Corbelletta Dott.ssa Daniela	v. C. Battisti, 19	Borgo val di taro
Farmacia Piazza	Piazza Dott. Fabrizio	V. Repubblica 17	Felegara
Farmacia Cardinali	Cardinali Dott.ssa Gabriella	v.le Libertà, 18	Borgo val di taro
Farmacia S.Alfonso	Lombardo Dr. Fabrizio	V. Roma 12	Bardi
Farmacia del taro	Munafò dr. Vincenzo	v. Nazionale, 82	Fornovo Taro
Farmacia S. Giorgio	Chiesi Carlos	via Nazionale 79/c	Collecchio
Farmacia Costella	Dott. Costella Corrado e Luca	p.zza Manara, 12	Borgo Val di Taro
Farmacia S. Maria Del Taro	FOROUHAR	NASHERI	Samts maria del Taro
Farmacia Comunale S.Maria Taro	Brandini Dr.ssa Cristina	p.za Lusardi, 21	S. Maria del Taro
Comune Pellegrino	Pirroni Sonia	V. Micheli, 1	Pellegrino P.se
Farmacia Pettenati	Frattini Dott. Amina	V.Roma 68	Medesano
Farmacia Leonardi	Leonardi Dott. Filippo	V. Martiri Libertà, 31	Varano de Melegari
Farmacia lorio	lorio Dott.ssa Maria	V. Fondovalle 16	Solignano
Comune Terenzo	Calza Silvana	loc. Terenzo	Terenzo
Comunita Alloggio di Mormola	Tassi Francesca	str. Provinciale mormorola 1	
Comune Berceto (Casa Protetta)	Guelfi, Pezzani	V. G. Marconi, 18	Berceto
Farmacia Chiappari	Chiappari Dott. Maria Rosa	Provinciale Sud 21	Tarsogno
Farmacia Bocchialini	Bocchialini Dott. Gianfranco	V. Garibaldi 4	Bedonia
Farmacia Compiano	Mancini Dott. Annamaria	V.Ponte 5	Compiano
Farmacia Maturo	Cimino Dr.ssa Giuseppina	V. Buca 72	Neviano degli Arduini
Farmacia Monchio	Musmeci Clementina	Via F. Bocchialini 2	Monchio delle Corti
Farmacia Bracchi	Bracchi Dott. Gian Antonio	V. Carducci 1 lla	Felino
Farmacia Dedali	Dedali Corrado	via Matteotti 28	Montechiarugolo
Farmacia S. Michele	Pinotti Dr.ssa Maria	v. Alighieri, 6/b	S. Michele Tiorre
Comune Calestano	Benedetto Federica	v. Mazzini,18	Calestano
Comune Montechiarugolo	Dacci, Carra	P. Rivasi, 3	Basilicanova
Farmacia Agnelli	Agnelli Dott. Umberto	V. Argini, 28	Lesignano Bagni (PR)
Farmacia Ghiare di Corniglio	Bandini Dott. Claudia	Str. Provinciale 6/a	Ghiare di Corniglio
Farmacia Comunale Pastorello	Urbani Dott. Marilena	Strada Monchio 9/b	Pastorello di Langhirano
Farmacia Comunale di Scurano	Fadani Dr.ssa Nicoletta	Scurano	Scurano
Farmacia Lonetti	Lonetti Dott. Antonio	P.za Rustici 10	Corniglio
Farmacia Chehade	Chehade Dott. Salah El Din	V.le Europa Unita 8	Tizzano
Farmacia Comunale Pastorello	Urbani Dott. Marilena	Strada Monchio 9/b	Pastorello di Langhirano
Farmacia Rizzoli	Rizzoli Dott. Francesca	P.za Veneto 41	Traversetolo
Farmacia Dei Bono	Pontillo Dr.ssa Giuseppa	V. Mazzini 25	Langhirano
Farmacia S. Rita	Pasini Dott. Francesca	V. Parma 26	Basilicagoiano
Comunita Montana	Branchi Barbara	via parco dei cento laghi 4	Monchio delle Corti
Farmacia Comunale Lagrimone	Bocchi Dr.ssa Simona	loc. Lagrimone	Lagrimone

Farmacia Ferri	Ferri Dr.ssa Emilia	v. Provinciale	Palanzano
Farmacia S. Maria delle Grazie	Maria Teresa vecchia	via M. libertà 100	Mezzani inf.
Comune Roccabianca	Barbarini Angela	v.le Rimembranze, 3	Roccabianca
Comune Trecasali	Canu Giovanna	V. Nazionale, 50	Trecasali
Farmacia S. Antonio	Melegari Dott. Andrea	P.za Ferrari 4/a	Sissa
Farmacia Sorbolo Dr.Busani	Busani	Via Italo Focherini, 11	43058
AVIS Sorbolo	Cantoni, Frigeri, Bellanova	V. Gruppini	Sorbolo
Farmacia Amadei	Amadei Dott. Mario	V. Matteotti 361a	Sissa

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0303

Oggetto : Elenco Trattamenti

Data Ultima Modifica :20/03/2009

REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI

(Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione di dati personali)

Elenco dei trattamenti di competenza delle Aziende Sanitarie

1. Tutela dai rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro
2. Profilassi generale delle malattie infettive e diffusive e delle tossinfezioni alimentari: sorveglianza epidemiologica
3. Profilassi specifica delle malattie infettive e diffusive - vaccinazioni e verifica assolvimento obbligo vaccinale
4. Programmi di diagnosi precoce
5. Attività fisica e sportiva
6. Gestione attività sociosanitaria a favore di fasce deboli – disabili adulti e minori
7. Medicina di base - pediatria di libera scelta - continuità assistenziale (guardia medica notturna e festiva, guardia turistica)
8. Assistenza sanitaria di base: riconoscimento del diritto all'esenzione per patologia/invalidità/reddito e gestione archivio esenti
9. Assistenza sanitaria di base: assistenza sanitaria in forma indiretta
10. Assistenza sanitaria di base: cure all'estero
11. Assistenza sanitaria di base: assistenza agli stranieri in Italia (particolari categorie)
12. Assistenza integrativa (fornitura di prodotti dietetici a categorie particolari e di presidi sanitari a soggetti affetti da diabete mellito).
13. Assistenza protesica
14. Assistenza domiciliare programmata e integrata
15. Attività di assistenza riabilitativa residenziale e semiresidenziale ad anziani non autosufficienti, disabili psichici e sensoriali e malati terminali
16. Assistenza termale
17. Assistenza in regime di ricovero ospedaliero e domiciliare
18. Attività immuno-trasfusionale
19. Trapianti
20. Soccorso sanitario di emergenza/urgenza sistema "118". Assistenza sanitaria di emergenza
21. Assistenza specialistica ambulatoriale e riabilitazione
22. Promozione e tutela della salute mentale
23. Dipendenze (tossicodipendenze e alcoodipendenze)
24. Assistenza socio-sanitaria per la tutela della salute materno-infantile
25. Esiti della gravidanza: nascita, aborto spontaneo, interruzione volontaria della gravidanza
26. Assistenza farmaceutica territoriale e ospedaliera
27. Sperimentazione clinica dei medicinali
28. Farmacovigilanza e rilevazioni reazioni avverse a vaccino
29. Autorizzazione alla importazione dei farmaci non registrati in Italia per utilizzo su singolo paziente
30. Erogazione a totale carico del servizio sanitario nazionale, qualora non vi sia alternativa terapeutica valida, di medicinali inseriti in apposito elenco predisposto dalla commissione unica del farmaco
31. Produzione di medicinali su ricetta medica da parte di aziende farmaceutiche
32. Assistenza a favore delle categorie protette (Morbo di Hansen)
33. Malattie rare
34. Assistenza ai nefropatici cronici in trattamento dialitico
35. Attività medico - legale inerente l'istruttoria delle richieste di indennizzo per danni da

vaccinazioni obbligatorie, trasfusioni e somministrazione di emoderivati

36. Attività medico-legale inerente gli accertamenti finalizzati al sostegno delle fasce deboli (riconoscimento dello stato di invalidità civile, cecità civile, sordomutismo, della condizione di handicap, accertamenti per il collocamento mirato al lavoro delle persone disabili)
37. Attività medico - legale inerente l'accertamento dell'idoneità in ambito di diritto al lavoro (assunzione nel pubblico impiego; idoneità allo svolgimento di mansioni lavorative; controllo dello stato di malattia di dipendenti pubblici e privati)
38. Attività medico - legale inerente l'accertamento dell'idoneità al porto d'armi, ai fini della sicurezza sociale
39. Attività medico - legale inerente l'accertamento dell'idoneità alla guida, ai fini della sicurezza sociale
40. Consulenze e pareri medico-legali in tema di riconoscimento della dipendenza da causa di servizio
41. Consulenze e pareri medico-legali in tema di ipotesi di responsabilità professionale sanitaria, di supporto all'attività di gestione del rischio clinico, informazione e consenso ai trattamenti sanitari
42. Attività medico - legale in ambito necroscopico
43. Registri e studi epidemiologici
44. Gestione del rapporto di lavoro con il personale dipendente
45. Gestione contenzioso legale (compreso gestione esposti utenti)
46. Gestione e verifica sull'attività specialistica e di ricovero delegata alle strutture accreditate

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0703

Oggetto : Regolamento per l'utilizzo degli strumenti informatici dell'Azienda USL di Parma

Data Ultima Modifica:23/04/2013

1. Introduzione

La gestione dei processi dell'Azienda USL di Parma è prevalentemente basata su strumenti informatici. Il punto d'accesso principale è la stazione di lavoro, generalmente composta da un Personal Computer (fisso, portatile, palmare, ecc.) e da eventuali periferiche (stampante, unità dischi esterne, ecc.).
L'utilizzo della stazione di lavoro avviene in ambito locale (es. creazione e salvataggio su disco di documenti, fogli di lavoro, ecc.) e/o in rete aziendale (es. Intranet, posta elettronica, procedure aziendali, ecc.). In entrambi i casi l'utilizzo è sottoposto alla normativa vigente in materia di trattamento dei dati e sicurezza degli stessi (D.lgs 196/2003 “Codice sulla Privacy”). Il presente regolamento ha come finalità quella di garantire un corretto utilizzo del sistema informatico per gli scopi istituzionali assicurando, nel contempo, il rispetto della normativa citata.

2. Ambito di applicazione e requisiti

2.1 L'Azienda USL, attraverso il Servizio Risorse Informatiche e Telematiche (S.RIT), recepisce i seguenti criteri in merito alla gestione e fruizione dei propri dati da parte degli utenti:

a) Confidenzialità - I dati non devono essere accessibili ai non aventi diritto

b) Integrità - Non deve essere possibile alterare i dati

c) Disponibilità - I dati devono essere sempre disponibili agli aventi diritto

2.2 Al fine di gestire un sistema “sicuro”, è necessario che gli utenti abbiano ricevuto formazione adeguata e che siano informati sui rischi di una cattiva gestione dei sistemi. Si assume perciò che l'atteggiamento sia ispirato alla correttezza ed alla buona fede, restando valida in ogni caso l'assunzione di responsabilità personale per le attività svolte.

2.3 L'adozione del presente regolamento è finalizzata a:

a) fornire la massima disponibilità ed efficienza del servizio nell'interesse della produttività aziendale;

b) garantire la massima sicurezza possibile nell’accesso alla rete privata (Intranet) e pubblica (Internet);

c) garantire il rispetto delle leggi in materia di “Tutela della Privacy” attraverso un utilizzo lecito delle risorse informatiche per l’elaborazione di dati personali e sensibili;

d) provvedere ad un'efficiente attività di monitoraggio e controllo a fini diagnostici ed evolutivi .

2.4 E' vietato l'uso delle risorse informatiche aziendali per tutte le attività illegali e quelle:

a) commerciali o a fini di lucro;

b) personali che sottraggano risorse al sistema aziendale;

c) che possono rappresentare una violazione della legge in materia di Copyright e Licenza d'uso, fra le quali la copia non autorizzata di software brevettato e/o protetto;

d) che compromettono in qualsiasi modo la sicurezza delle risorse;

e) non conformi alla normativa sulla privacy.

2.5 Il presente regolamento è applicabile a tutti coloro che accedono alle risorse informatiche aziendali. L’accesso a tali risorse è riservato ai dipendenti dell’Azienda USL di Parma e a coloro che, a seguito di atti aziendali, hanno acquisito il diritto di accesso. Si assume che:

a) l'Azienda USL di Parma adotta il principio secondo il quale ogni strumento informatico deve essere utilizzato dall'utente per i soli scopi istituzionali per cui è stato implementato, perciò le attività di monitoraggio e controllo di detti strumenti non intendono violare la privacy dell'utente interessato;

b) ogni azione non conforme al presente regolamento verrà considerata una violazione della sicurezza e, come tale, comporterà la revoca dell'accesso alle risorse informatiche e la segnalazione al Responsabile; i casi più gravi (che violino anche la legislazione vigente) verranno segnalati all'Autorità competente e potranno essere soggetti ad azioni disciplinari o legali;

c) considerata la dinamicità tecnologica e legislativa dell'argomento trattato, occorre considerare il presente regolamento come elemento dinamico, quindi soggetto ad aggiornamenti periodici; perciò l'utente è tenuto a prendere visione e accettare anche gli eventuali aggiornamenti che verranno pubblicati sulla pagina Intranet aziendale (http://intra.ausl.pr.it); il presente documento va considerato come parte integrante della normativa vigente in materia di sicurezza informatica, che ogni utente è tenuto a conoscere e rispettare.

3. **Regole di comportamento e utilizzo delle risorse**

3.1 Stazione di lavoro (Personal Computer, periferiche, software)

a) L'utente risponde del buon uso della stazione di lavoro che gli è stata affidata, comprese le eventuali periferiche associate e il software preinstallato. In particolare è responsabile dell'installazione del SW, specie se sprovvisto di regolare licenza. Qualsiasi software fornito dall'utente (anche se prelevato da siti Internet o in allegato a riviste e libri o in dotazione a periferiche specifiche) deve installato e utilizzato dietro approvazione del S.RIT. E' proibito l'uso di software Peer to Peer, Instant Messaging e Chat.

b) L'utente è tenuto a utilizzare in modo ottimale la dotazione software standard, per utilizzare la quale può richiedere eventualmente l'inserimento in piani di attività formativa aziendale pianificata.

c) L'utente è obbligato a disconnettere la sessione corrente quando la stazione di lavoro rimane non presidiata, per salvaguardarla da accessi indesiderati.

d) L'utente è tenuto a presidiare adeguatamente le proprie stampe prodotte dalle stampanti in rete, in particolar modo se contengono dati sensibili.

e) L'utente deve sottoporre a scansione antivirus i files acquisiti nella stazione di lavoro attraverso le diverse tipologie di trasferimento (dischetto, porta USB, CD, ecc).

f) Se l'utente viene autorizzato come Amministratore Locale del Personal Computer (es: programmi che non funzionano in ambienti con diritti "User") diventa automaticamente responsabile di ogni cosa che avviene da/su detta postazione essendo in grado di accedere con pieno controllo al sistema; ad esso viene assegnata la responsabilità di perdita/abuso di dati o "attacchi" informatici perpetrati tramite quel sistema.

g) Ogni utente che ne abbia necessità può richiedere di inserire in rete un sistema di sua proprietà, dietro richiesta scritta e avvallo da parte della Direzione del servizio di appartenenza e dietro parere tecnico del S.RIT, rimanendo comunque responsabile delle manutenzione HW/SW preventiva/correttiva e di ogni danno cagionato tramite il sistema stesso. Il S.RIT si riserva la possibilità di effettuare controlli su tale sistema.

h) E' vietato cablare o collegare apparecchiature (di qualsiasi natura e tipo) alle prese di rete senza l'autorizzazione del S.RIT, modificare le impostazioni predefinite e assegnate dal S.RIT, installare modem configurati per l'accesso remoto, intraprendere azioni allo scopo di degradare le risorse del sistema e impedire ad

utenti autorizzati l'accesso alle risorse, effettuare copie di file di configurazione del sistema operativo.

i) E' vietato diffondere software prelevato da infrastrutture aziendali al di fuori dei termini delle licenze, diffondere software che possa danneggiare le risorse informatiche, accedere a dati e/o applicativi per i quali non si è ricevuta esplicita autorizzazione o incarico.

3.2 Rete, modalità di accesso (Posta elettronica, Internet, Intranet) e protezione dei dati

a) L'accesso alle risorse avviene mediante un identificativo (account, ovvero user/utente e password, ovvero smart card) strettamente personale e non cedibile ad altri; in ogni caso l'utente viene considerato responsabile di eventuali atti illeciti perpetrati con il proprio account.

b) L'utente deve proteggere il proprio account mediante password nel rispetto della normativa vigente (lunghezza minima della password, modifica periodica, utilizzo di caratteri numerici e maisucoli/minuscoli).

c) L'utente è responsabile della protezione e dei salvataggi periodici dei dati utilizzati e/o memorizzati nei sistemi nei quali ha accesso, ad eccezione di quelli memorizzati su sistemi centralizzati, al cui salvataggio periodico sovrintende il S.RIT.

d) E' responsabilità dell'utente segnalare al una prolungata assenza (per comando, maternità, ecc…ecc…) per poter bloccare l'account ed evitare possibili abusi.

e) Il contenuto e la manutenzione della casella di posta elettronica è posta sotto la diretta responsabilità dell'utente, compresa la verifica di eventuali messaggi malevoli (phishing), allegati infetti (virus), propagazione di messaggi indesiderati (spam).

f) Non è permesso l'invio di dati personali o sensibili tramite posta elettronica se non preventivamente autorizzati dalla direzione di competenza; è comunque vivamente sconsigliato l'uso della posta elettronica per l'invio di dati rilevanti verso utenti esterni, poiché il transito sulla rete Internet è in "chiaro" e quindi potenzialmente leggibile da qualsiasi utente collegato alla rete Internet.

g) E' permesso l'accesso a siti che forniscono servizi gratuiti di Posta Elettronica esclusivamente in modalità Web (protocollo http).

h) L'utente è personalmente responsabile della violazione degli accessi protetti e dei contenuti prelevati in rete Internet. Il S.RIT ha la facoltà di interrompere il collegamento degli utenti qualora il sito visitato sia ritenuto in contrasto con i principi del servizio pubblico o lesivo della dignità della persona.

i) Non è permesso l'invio di dati personali o sensibili tramite la rete internet (Upload) se non preventivamente autorizzati dalla direzione di competenza.

j) Non è permesso l'utilizzo della rete Internet per Instant Messaging, Chat, telefonate virtuali e Stazioni Radio/Video, se non preventivamente autorizzati e configurati dal S.RIT.

k) Non è consentita l'installazione e l'utilizzo di programmi di file sharing (condivisione).

l) Non è consentita la memorizzazione/consultazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica,opinione e appartenenza sindacale e/o politica.

m) E' vietato utilizzare strumenti/procedure di rete di esclusiva pertinenza del S.RIT, come cracker o software di monitoraggio della rete, configuratori di servizi centralizzati (quali DNS-Domain Name Service, DHCP-Dynamic Host Configuration Protocol, NTP-Network Time Protocol, LDAP, mailing, Web Server, accesso remoto

o dial-up); installare apparecchiature di rete (quali Switch, Hub, Access point ecc… ecc..) , effettuare operazioni di routing/bridging/tunneling, intercettare pacchetti sulla rete utilizzando “Sniffer” o software analoghi.

n) E' vietato divulgare i numeri telefonici e le password dei modem aziendali.

3.3 Controllo e monitoraggio

a) Il Sistema di monitoraggio (Amministrazione del sistema) opera nel rispetto delle politiche adottate dall’Azienda USL di Parma in materia di sicurezza, al fine di garantire la massima riservatezza/disponibilità/integrità nei trattamenti dei dati personali e sensibili.

b) L’Azienda USL di Parma si è dotata di uno strumento per il controllo degli accessi Internet. Tale strumento non garantisce l’inaccessibilità totale a siti non istituzionali o a rilevanza penale, di conseguenza la responsabilità della navigazione è totalmente a carico dell’utente.Il S.RIT e/o gli amministratori di sistema si riservano il diritto di revocare l'accesso alle risorse senza preavviso, qualora essi siano utilizzati impropriamente o in violazione delle leggi vigenti.

c) Gli Amministratori di Sistema devono essere in grado in qualsiasi momento, specialmente in caso di emergenza, di poter accedere ai locali e ai Sistemi loro affidati;

d) Gli accessi vengono registrati nel tempo attraverso opportuni log di sistema e i controlli possono essere fatti al momento e/o a campione dal S.RIT, oppure in tempi successivi. Qualsiasi comportamento ritenuto non ammissibile alla luce dei regolamenti verrà segnalato alla Direzione Aziendale e/o alle Autorità Competenti.

e) Gli Amministratori di Sistema, dietro richiesta esplicita del Responsabile e/o del Titolare del trattamento dati, possono accedere ai Sistemi per scopi di monitoraggio e controllo del corretto utilizzo del sistema stesso da parte dell’utente.

f) Gli Amministratori di Sistema, dietro richiesta esplicita del Responsabile e/o del Titolare del trattamento dati, possono accedere ai dati sui Sistemi Informatici per garantire la continuità del servizio garantendo la riservatezza del singolo utente.

g) Gli Amministratori di Sistema possono provvedere senza preavviso (in caso di emergenza da attacco informatico o da “Virus”), all’aggiornamento Software di tutte le postazioni anche se questo prevede un immediato riavvio dell’elaboratore. Gli utenti sono invitati a segnalare al S.RIT l’elenco di quegli elaboratori che devono essere riavviati in modo presidiato per evitare disservizi.

h) Gli Amministratori di Sistema, dietro richiesta esplicita del Responsabile e/o del Titolare del trattamento dati, possono accedere al personal computer e al sistema di messaggistica per scopi di monitoraggio/controllo o continuità di servizio.

i) Gli Amministratori di Sistema e i Tecnici di Supporto, possono accedere al personal Computer (anche senza preavviso) per manutenzione preventiva e correttiva.

3.4 Standard aziendali e accesso al Servizio RIT

Lo standard aziendale prevede l'utilizzo di software aderente alle normative in merito al Codice Digitale della P.A. L'Azienda utilizza formati di documenti (testo, foglio elettronico, ecc.) aperti (open) e, quando non sia richiesta possibilità di modifica, viene privilegiato il PDF (Portable Document Format). Gli utenti sono tenuti a comunicare agli interlocutori istituzionali queste istanze e, nel caso si verifichino incompatibilità di formati, devono comunicare al S.RIT il problema incontrato in modo dettagliato, riproducibile e fornire i riferimenti dell'interlocutore.

L'accesso al S. RIT deve avvenire prevalentemente attraverso l'help desk, attivato via Intranet, tramite mail o attraverso una chiamata al call center rispondente al 3931 che garantisce la tracciabilità della chiamata. Esiste una lista di utenti V.I.P. (Direzione, Direttori di Distretto, di Presidio, di Dipartimento etc etc) secondo organigramma aziendale, che potrà essere reindirizzata direttamente alle risorse interne del S.RIT. L'Helpdesk fornisce risposte a quesiti specifici o richieste di assistenza, riguardanti le infrastrutture informatiche, l'utilizzo degli applicativi e la fornitura di dati. Per ottimizzare e tracciare le richieste si adotta un flusso ad elevato grado di informatizzazione, che prevede come modalità di accesso la pagina Intranet, la mail, la chiamata al call center. Viene posta attenzione sul fatto che la richiesta telematica segue un percorso ottimizzato.L'attività di helpdesk, in particolare per quanto riguarda il supporto sugli applicativi, deve essere in grado di filtrare eventuali richieste non pertinenti, ovvero di natura funzionale/applicativa anzichè informatica, veicolandole verso le sedi opportune. L'attività di helpdesk deve consentire una rapida presa in carico delle richieste e una rapida individuazione di competenza, che può prevedere quattro possibili uscite:

1.Attribuzione a uno specialista interno (con possibile attivazione di fornitori o specialisti esterni)
2.Attività a campo (svolta dal fornitore di servizio di supporto HW)
3.Attribuzione alla U.O. Aziendale di riferimento dell'attività
4.Richiesta non pertinente

Il supporto alle procedure applicative, come attività di helpdesk, è rimandato alle funzioni aziendali referenti per area tematica.

4. Sanzioni

In caso di violazione delle regole sopra citate e a seconda della gravità delle medesime, fatte salve le ulteriori conseguenze di natura penale, civile e amministrativa (Esempio: Titolo III D.lgs 196/2003), possono essere comminate le seguenti sanzioni:

k. richiamo verbale;

l. richiamo scritto;

m. segnalazione alla Commissione Disciplinare Aziendale.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0304

Oggetto : Elenco Server Aziendali

Data Ultima Modifica : 23/04/2013

Di seguito l'elenco dei server aziendali installati presso la sala server all'Ugolino in strada del Quartiere 2/A

Modello	Serial Number	Nome Server	Utilizzo
IBM x345	551214M	PROXYAUSL1	Server Proxy
IBM x345	551209R	BACKUPSERVER	Server di Backup EMC Legato Networker
IBM x345	551216A	FSECURE	Server Antivirus-Susupdate-CUP Telefonico
IBM x345	551213D	GPITEST	DBServer TEST GPI
IBM x345	551212P	NEWTSSAN	Terminal Server Sanitario
IBM x345	551213F	x345_DF	Server Intranet
IBM x345	551211N	NACSERVER	Server autenticazione NAC
RX300S4	YKAF023445	ESX1	ESX hosts
RX300S4	YKAF023442	ESX2	ESX hosts
RX300S4	YKAF023447	ESX3	ESX hosts
RX300S4	YKAF023446	ESX4	ESX hosts
RX300S4	YKAF023444	ESX5	ESX hosts
RX300S4	YKAF022677	DBZEN	Zensistemi
RX300S4	YKAF022720	ESX7	ESX hosts
RX300S4	YKAF022659	ESX6	ESX hosts
RX300S4	YKAF023366	DBPERSONALE	DB Server Personale
RX300S4	YKAF023365	ASPERSONALE	Application Server Personale
NEC EXPRESS 5800	100013721128	SRVWEBTAX	server WEBTAX per registrazione call telefoniche
HP Proliant DL385 G6	CZC9313QXQ	PACSFED	PACS Federale (CUP2000)
PoweEdge 1850	7SK9F1J	ITACA1	DBServer Itaca (cluster)
PoweEdge 1850	6SK9F1J	ITACA2	DBServer Itaca (cluster)
PoweEdge 1850	7WK9F1J	AMMINISTRATIVO	DBServer Bilancio
PoweEdge 1850	9SK9F1J	PROXYVADP	Proxy VADP per backup VM
PoweEdge 1850	3HCBF1J	DPS	Server DPS
PoweEdge 1850	HSK9F1J	PROXYWOL	Proxy Wake On Lan
PoweEdge 1850	CSK9F1J	JBOSS_OLD	Appl. Server Bilancio
PoweEdge 1850	BSK9F1J	SERVER.RETE	DHCP+DNS
PoweEdge 1850	GSK9F1J	VPNAVEN	server VPN verso AVEN (IPSec)
PoweEdge 1850	8SK9F1J	DNSEXT	DNS + Spazio Giovani
PoweEdge 1855	8FQLF1J	ASS1	Appl. server procedure sanitarie ADS
PoweEdge 1855	5FQLF1J	ASS2	Appl. server procedure sanitarie ADS
PoweEdge 1855	3FQLF1J	ASS3	Appl. server procedure sanitarie ADS
PoweEdge 1855	GFQLF1J	ASS4	Appl. server procedure sanitarie ADS

PoweEdge 1855	JDQLF1J	ASS5	Appl. server procedure sanitarie ADS
PoweEdge 1855	DDQLF1J	ASS6	Appl. server procedure sanitarie ADS
PoweEdge 1855	FQSHG2J	ASRUR	AS Server applicativo RUR (Invalidi civili)
PoweEdge 1855	GQSHG2J	OPENVPNNEW	Server per accesso via OpenVPN
PoweEdge 1855	DQSHG2J	PARMA.SFERACARTA.COM	Server applicativo "Sferacarta"
PoweEdge 1855	9BQLF1J	DBProtocollo	DB procedura Protocollo
PoweEdge 1855	BCQLF1J	ASProtocollo	Appl. server procedura Protocollo
PoweEdge 1855	DBQLF1J	ASITACA1	Appl. server procedura Itaca
PoweEdge 1855	CQSHG2J	NAGIOS1	Server per monitoraggio rete (Nagios, …)
PoweEdge 1855	1DQLF1J	BDSOLEDB	DB server progetto BSole
PoweEdge 1855	H9QLF1J	ASITACA2	Appl. server procedura Itaca
PoweEdge 1850	DSK9F1J	DBRUR	DB Server applicativo RUR (Invalidi civili)
IBM x3950	99T0742	europa	DB Server Sanitario (Cluster primario, nodo principale)
IBM x336	KDRDZB6	ganimede	DB Server Sanitario (Cluster primario, nodo secondario)
IBM x346	KKRXG5V	serverltt	Server Intranet LTT
IBM x346	KKRXG9W	gescel	Server Gestione Celiaci (DB + A.S.)
DD630	1FZ0413004	DD630	unità di backup Data Domain 630
ACER AR385FI	SRR8HEE0012410002B9700	PARMADB1	db Server Veterinari (Sferacarta)
IBM x345	551168T	DBZEN2K3	DB Server Zen Sistemi (temporaneo)
HP ProLiant DL380 G6	CZ202375L6	PROXY1	Server proxy DMZ
IBM x3650	KDWHWTC	PARMADB	DB Server Veterinari (Sferacarta)
IBM x3650	KDWKKCC	PARMAWEB	Application Server Veterinari (Sferacarta)
Fujitsu Siemens RX600 S6	YL6T028514	RISPRDB1	DB Server RIS nodo 1
Fujitsu Siemens RX600 S6	YL6T028515	RISPRDB2	DB Server RIS nodo 2
HP ProLiant DL380 G6	CZ202688RP	SOLE1	DB Server
HP ProLiant DL380 G6	CZ202688RN	SOLE2	DB Server
HP ProLiant DL380 G6	CZ202688RX	PROXY2	Server proxy DMZ

IBM BC HS23	06LAPH7	MARTE	DB Server Sanitario
IBM BC HS23	06LAPH6	VENERE	DB Server Sanitario

Di seguito l'elenco dei server aziendali installati presso la sala server nell'Ospedale di Fidenza in via Don Tincati a Fidenza

HP ProLiant DL380 G4	GB85158NN0	SERVERPDF	Server generatore PDF
HP ProLiant DL380 G4	GB85158NNH	MULTIFUNC	Multifunzione
HP ProLiant DL380 G4	GB85158NNB	WINDOPATH	Server applicativo Windo Path

HP ProLiant DL380 G4	GB85158NNT	VMWAREFID	Host VMWare Server
HP ProLiant DL380 G4	GB85158NN5	DNLAB1	Cluster DNLAB laboratorio (nodo 1)
HP ProLiant DL380 G4	GB85158NN2	DNLAB2	Cluster DNLAB laboratorio (nodo 2)
ACER AR385FI	SRR8HEE001241000299700	PROXYFID1	proxy Internet
ACER AR385FI	SRR8HEE001241000289700	PROXYFID2	proxy Internet

Di seguito l'elenco dei server aziendali installati presso l'Ospedale di Borgo val di Taro in via Benefattori a Borgo val di Taro

Fujitsu-Siemens RX600	SSAN101610	DNLABBGT	DB server DNLab
ACER AR385FI	SRR8HEE001241000229700	PROXYBOR1	proxy Internet
ACER AR385FI	SRR8HEE001241000279700	PROXYBOR1	proxy Internet

Di seguito l'elenco dei server installati nell'ambiente virtuale VMWARE

3pstudiovm	server applicativi 3Pstudio
anagrafesole	Application server Anagrafe Sole
asdedalus	AS Server applicativi Dedalus
aseurosoft1	Application Server Eurosoft
aseurosoft1test	Application Server Eurosoft (test)
aseurosoft2	Application Server Eurosoft
aseurosoft3	Application Server Eurosoft
aszen1	Application Server Zensistemi
aszen2	Application Server Zensistemi
ausldom	Dominio di rete, LDAP slave, PDC
ausldomtest	Dominio di rete, LDAP slave, PDC (per test e collaudo)
bdcpr	Backup Domain Controller PR
carcere	applicativo Carcere CCI
cardioline	Raccoglitore ECG e prove da sforzo (Fidenza)

cassaedile	Cassa Edile
dbdedalus	DB Server applicativi Dedalus
dbrurtest	DB Server applicativi RUR-ER di TEST
egate	server applicativo eGate (Itaca)
esrsgw	EMC Secure Remote Support Gateway
etichette1	ISEE Etichette
etichette2	ISEE Etichette
eurotouch	Server applicativo Eurotouch
farmadati	Server applicativo Farmadati
federaidp	server IdP per progetto Federa
firmadigitale	postazione Firma Digitale Borgotaro
fsecure9	Console Antivirus F-Secure 9
guatemala	PC di test Luca
igconsulting	Server DSS (IGConsulting)
imed	server applicativo iMed
itaca-AS-test	AS test Itaca
itaca-DB-test	DB test Itaca
jboss	Appl. Server JBOSS
jpdfwriter	JPDFWriter: generatore PDF
lamp	Server Linux, Apache, MySQL, PhP
lampext	Server Linux, Apache, MySQL, PhP (per esterni)
lamptest	Server Linux, Apache, MySQL, PhP
ldapserver	Server LDAP master, Rap3
logserver	Log server Splunk
logserverOLD	Log server Splunk
mail	server di posta Zimbra
mobilitystat	Portale Statistiche Mobilità

ocs	OCS Inventory + OTRS
otrs	server OTRS 3
paf	Piano Formativo Aziendale
parer	server applicativo Parer
pensioni	Server applicativo Pensioni
pensioninew	Server applicativo Pensioni (nuovo aggiornato)
pentaho	applicativo Pentaho
profis	Server applicativo Profis
proxyausl	server Proxy Internet
qlik	Reportistica Direzionale
radius	server autenticazione Radius
remotecheckads	server di raccolta dati per remote checking ADS
repobackup	repository dei backup
repository	Repository aziendale di rete
reverseproxy	Reverse Proxy
rispras1	Appl. Server RIS
rispras2	Appl. Server RIS
risprprint	Integrazioni Elco con sistemi esterni
risprvoc	riconoscimento vocale RIS
serveriap	Server Applicativo IAP (numero verde)
serverlunghi	Server applicativi Lunghi
sister	Server progetto SISTER
sondaggio	Portale Questionario Intranet/Internet (Fabio/Thomas)
susupdate	Susupdate 3
energybrain	sistema monitoraggio Energy Brain (Fidenza)
test-auth	test per autenticazione SSH-PAM-LDAP
tsserver	Server Servizi Terminal
tstao	Terminal Server TAO (+Gepadial)
urologiafid	server applicativo Urologia (ex benecchi)
vcenter	Virtual Center 5

wiki	Wiki Ausl
win2k8test	macchina Windows 2008 per i test
win7test	macchina Windows 7 per i test
win2k12test	macchina Windows 2012 per i test
winxptest	macchina Windows XP per i test
zenoss	sistema monitoraggio server Oracle
win2k3test	macchina Windows 2003 per i test
win8test	macchina Windows 8 per i test
helicswin	applicativo HELICSwin: raccolta dati prevernzione malattia
bct	server centralino BCT
webtax	server WEBTAX per registrazione call telefoniche
geriatria	Server applicativi Lunghi Osservatorio Geriatria
radiance	applicativo Radiance per Emogasanalizzatori
asprototest	as protocollo di test
asprotocollo	asprotocollo
radius_test	test radius
risprweb	application server RIS
gammacompmd	Server GammaComMD calibrazione monitor medicali NEC
alfresco	server documentale Alfresco
busterspid	monitoraggio armadi farmaci Fidenza
parma58temp	test su applicativo Parma 5.8
assanadsias_test	test application server iAS Sanità
assanadstomcat_test	test application server Tomcat Sanità
adsias1	application server iAS Sanità
adsias2	application server iAS Sanità
adsias3	application server iAS Sanità
adstom1	application server Tomcat Sanità
adstom2	application server Tomcat Sanità
adstom3	application server Tomcat Sanità
adsbridge	macchina ponte per ADS

intranetdps	server Intranet DPS
dbigc	DB Server IGConsulting
qlikserver	QLIK server - reportistica aziendale
bsoleas	AS server progetto Bsole CUP2000

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0103

Oggetto : Regolamento AVEN

Data Ultima Modifica :20/03/2009

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Area Vasta Emilia Nord

AVEN

Disciplinare sull'utilizzo degli strumenti aziendali e istruzioni in materia di trattamento dei dati personali

*Il presente documento costituisce un disciplinare sull'utilizzo delle attrezzature informatiche e di telecomunicazioni aziendali ai sensi di quanto previsto al punto 3.2 delle "**le linee guida del Garante per posta elettronica e internet**"*

Sommario

Premessa

Il trattamento dei dati personali deve svolgersi " nel rispetto dei ***diritti e delle libertà fondamentali****, nonché della* ***dignità*** *dell'interessato, con particolare riferimento alla* ***riservatezza****, all'****identità personale*** *e al diritto alla* ***protezione*** *dei dati personali"*

Da tale enunciazione del Codice della Privacy (D.lgs.196/03) derivano una serie di obblighi in capo a chiunque utilizzi dati personali, non soltanto obblighi di riservatezza e segretezza ma anche di tutela, protezione e sicurezza dei dati.

I principi contenuti nel Codice della Privacy devono essere conosciuti e rispettati da chiunque tratti, nell'esercizio delle proprie funzioni, dati e informazioni personali e sensibili.*

* Il testo integrale del Codice Privacy è consultabile sulla intranet aziendale nella sezione speciale dedicata alla privacy (vedi in particolare il Titolo V "Trattamento di dati personali in ambito sanitario)

Il presente documento, che è stato redatto tenendo conto delle indicazioni contenute nel provvedimento del Garante per la protezione dei dati personali del 01/03/2007, bollettino n. 81 del marzo 2007, ha lo scopo di agevolare la lettura e l'interpretazione della normativa, dettando le necessarie prescrizioni e fornendo istruzioni operative.

Le istruzioni riportate si rifanno alla normativa in materia di protezione dei dati personali, alla normativa sul crimine informatico e più in generale al corpo normativo che disciplina i rapporti di lavoro.

L'azienda garantisce che per nessuna ragione i dati informatizzati gestiti dall'azienda, i sistemi di elaborazione dati e gli strumenti di telecomunicazioni saranno utilizzati per il controllo a distanza dei lavoratori (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n.300)

Il documento opera nei confronti di ogni dipendente dell'Azienda e di tutti coloro che a vario titolo si trovino ad utilizzare il sistema informativo dell'Azienda. Nel seguito del presente documento, per semplicità espositiva, si farà riferimento genericamente all'operatore.

Versioni più aggiornate del presente documento potranno essere reperite sulla intranet aziendale all'indirizzo: http://www...
Sarà cura dell'operatore accertarsi se siano state pubblicate nuove versioni della presente linea guida e adottare comportamenti congrui a quanto prescritto relativamente ai propri ambiti specifici di competenza e di attività. Una copia del presente documento sarà depositata presso l'ufficio _____ per poterne prendere visione e ottenerne copia.

È comunque indispensabile che chiunque tratti dati personali o sensibili prenda visione del vigente DPS – Documento Programmatico sulla Sicurezza –. Copia del DPS è reperibile presso l'ufficio _____ o sul sito WEB dell'Azienda nella intranet aziendale.

Istruzioni

Le seguenti istruzioni sono parte del sistema di sicurezza che l'Azienda _____ adotta al fine di gestire, nel rispetto della vigente normativa, i dati trattati.

Si sintetizzano di seguito alcuni aspetti particolarmente rilevanti in materia.

Accesso al sistema informatico aziendale e più in generale agli ausili tecnologici messi a disposizione dall'Azienda

NOTA BENE: le dizioni di seguito sottolineate costituiscono una formulazione alternativa. Ogni azienda potrà adottare la formulazione ritenuta più corretta

- *tutti coloro che per ragioni di lavoro devono avere accesso al sistema informatico aziendale devono*

essere intestatari di un nome di utente all'interno del dominio di sicurezza aziendale [e di un utente di posta elettronica], possono richiedere l'accesso [alla posta elettronica e] ad Internet che sarà autorizzato[i] o meno – in base alla mansione e a considerazioni organizzative – dal responsabile del trattamento di riferimento

- *la parola chiave di accesso alla postazione informatica e agli applicativi aziendali deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi*
- *la parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato*
- *a tutti gli utenti del dominio di sicurezza aziendale viene chiesto automaticamente ogni tre mesi il cambio della parola chiave; tuttavia, qualora si ritenga che la stessa non sia più sicura, è possibile sostituirla anche prima*
- *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*
- *l'incaricato è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare*

NOTA BENE: le indicazioni seguenti sottolineate possono essere diverse da azienda ad azienda.

- *per gli utenti del dominio aziendale è previsto un sistema di salvataggio dei files centralizzato, all'interno di file servers; i documenti gestiti all'interno dei file servers sono tutelati da perdite mediante accurate procedure di salvataggio; 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 al Servizio Informativo Aziendale*
- *in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni riservate o accedere alle banche dati, ad esempio scollegandosi o attivando un salvaschermo protetto da password*
- *è vietato manomettere o cambiare le configurazioni delle attrezzature aziendali se non esplicitamente autorizzati dai competenti servizi*
- *è vietato installare attrezzature non autorizzate e collegarle alla rete aziendale se non dietro esplicita autorizzazione dei servizi competenti*
- *è vietato intercettare/monitorare/ascoltare/leggere dati sulla rete di trasmissione dati o sulla rete di comunicazione in fonia*
- *il solo personale addetto alla manutenzione, al controllo e alla sicurezza delle infrastrutture tecnologiche è autorizzato a compiere le attività che garantiscano oltre al buon funzionamento delle infrastrutture aziendali il perseguimento dei fini istituzionali nei limiti e nel rispetto della normativa vigente*

- *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 –*

- *modalità da seguire per l'accesso ai dati in caso di prolungata assenza dell'incaricato – in ottemperanza a quanto prescritto al punto 10 dell'allegato B del d.lvo 196/2003 -:*

  - *è necessario distinguere due diversi casi a) il caso in cui i dati sono accessibili da più di un operatore b) il caso in cui i dati sono accessibili da parte di un unico operatore; nel caso in cui i dati siano accessibili da parte di più operatori – caso (a) - sarà necessario adottare le misure di seguito descritte solo nel caso in cui tutti gli operatori che hanno accesso ad un medesimo dato non siano presenti per un lungo periodo, per cui di seguito per semplicità si farà riferimento al solo caso (b):*
    - *nel caso in cui l'operatore che ha normalmente accesso al dato non possa per lungo periodo garantire ciò, sarà cura del responsabile del trattamento vicariare tale mancanza;*
    - *nel caso il responsabile del trattamento sia in grado di utilizzare le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, basterà che il responsabile del trattamento richieda al ___[indicare il servizio preposto alla gestione delle abilitazioni informatiche, normalmente il SIA]_____ le abilitazioni necessarie ad accedere al dato, una volta ricevute le abilitazioni opportune potrà accedere ai dati al posto dell'operatore assente; il responsabile del trattamento dovrà informare di ciò l'incaricato assente alla prima occasione utile;*
    - *nel caso il responsabile del trattamento non sia in grado di utilizzare direttamente le attrezzature e gli applicativi informatici normalmente utilizzati dall'operatore, farà richiesta al tecnico del _[indicare il servizio a cui afferiscono i tecnici che hanno in carico gli aspetti tecnici degli applicativi aziendali]__ che normalmente si occupa degli aspetti tecnici dell'applicativo di accedere ai dati necessari in qualità di incaricato temporaneo;*
    - *la misura precedente dovrà essere utilizzata solo nel caso l'urgenza lo richieda e nella misura strettamente necessaria a risolvere la situazione contingente, se l'esigenza va oltre la singola necessità e qualora i tempi lo consentano il Responsabile del trattamento disporrà di abilitare un diverso incaricato, in aggiunta a quello assente, all'accesso dei dati; il responsabile del trattamento dovrà informare di ciò l'incaricato assente alla prima occasione utile;*
    - *sarebbe opportuno che la individuazione di un diverso incaricato da abilitare all'accesso ai dati avvenisse da parte del responsabile all'interno di una rosa di fiduciari allo scopo previsti dall'incaricato; una tale gestione, se attuata, è in carico ai responsabili del trattamento;*
    - *le diverse richieste attinenti alla casistica descritta dovranno essere documentate da richieste scritte, eventualmente anche formulate via mail;*

Internet

- *è vietato l'utilizzo personale e non istituzionale della connessione a internet aziendale*
- *tutti gli <u>accessi ad Internet</u> vengono registrati sul sistema di sicurezza aziendale in appositi file di log; tali log tengono traccia dei seguenti dati per ogni accesso:*

  identificativo dell'utente che ha navigato in internet;
  identificazione della stazione di lavoro;

Data e ora
Riferimento al sito visitato (URL)

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 Informativo 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 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 al Servizio di Informatica 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) da quello centralizzato; NOTA BENE: questa affermazione sembra, in parte, in contrasto con la possibilità per l'operatore di consultare la propria posta elettronica personale via WEB.
  - 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;
  - produrre e pubblicare propri siti Web sulla infrastruttura tecnologica dell'Azienda; ogni eventuale necessità di realizzare siti Web personali o di struttura dovrà essere espressamente autorizzata dal Responsabile del trattamento dei dati;

Posta elettronica

- *è vietato l'utilizzo personale e non istituzionale della posta elettronica aziendale*
- *è 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*
- *il sistema di posta elettronica tiene traccia di tutte le e-mail inviate e ricevute*
  data e ora;
  identificativo della stazione di lavoro che ha inviato il messaggio;
  indirizzo di posta del mittente;
  indirizzo del destinatario;
  Anche in questo caso i log vengono mantenuti per lo stesso periodo e le stesse finalità indicate per gli accessi Internet

- *tutta la posta in transito sul sistema aziendale viene controllata da un sistema antivirus che, oltre a bloccare le e-mail con dei virus, effettua i seguenti controlli:*

Le seguenti NOTE TECNICHE sottolineate possono essere personalizzate dalle singole aziende:

j. blocco delle e-mail con allegati potenzialmente pericolosi (file con estensioni EXE, .COM, .VBS, .PIF, .SCR, .SYS, .BIN, .OVL, .DRV, .OVY, .LNK)

k. blocco delle e-mail con dimensioni complessive (messaggio di posta + allegati) superiori a 7 Mb.

l. blocco delle e-mail con più di 30 allegati e/o più di 50 destinatari.

m. in particolari situazioni, ad esempio massicce ricezioni di e-mail infette, il SIA 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 privatezza 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 favorisce la condivisione di indirizzi di posta elettronica fra più utilizzatori mediante l'adozione di cosiddette "maling list", cioè di gruppi di indirizzi;*
- *l'Azienda non fornirà indirizzi di posta elettronica aziendali per usi di tipo personale, ma non vieta la consultazione del contenuto di indirizzi di tipo personale, anche dall'interno dell'azienda, qualora la modalità di consultazione di tali informazioni sia compatibile con i vincoli di sicurezza del sistema aziendale e ciò avvenga in maniera non eccessiva e pregiudizievole degli obblighi del lavoratore nei confronti dell'Azienda;*

- *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 SIA di attuare la misura o attuarla in autonomia se tecnicamente 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 SIA l'adozione di una 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 alla locale sede del SIA 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 di Informativo Aziendale.

- *a titolo di esempio, senza che questo costituisca un elenco esaustivo, non è consentito:*
    - utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni non istituzionali o azioni equivalenti;
    - utilizzare il servizio di posta elettronica per inoltrare catene di S. Antonio, giochi, scherzi, barzellette e altre e-mail avulse dal contesto lavorativo.
    - 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;

Utilizzo dei sistemi di comunicazione in fonia – telefoni fissi, telefoni mobili, ecc… -

- *è 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 abbia la necessità di utilizzare, per fini istituzionali, una classe di numeri non abilitata potrà richiedere una specifica abilitazione*

- *per fini di controllo della <u>spesa telefonica</u> 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:*
    - *n. il numero del chiamante;*
    - *o. il numero chiamato;*
    - *p. 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;

- *l'utilizzo dei log dovrà in ogni caso essere compatibile con quanto prescritto dal d.lg. 13 maggio 1998, n. 171 "Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica"*

Ulteriori istruzioni per la tutela delle informazioni gestite dagli operatori

Documentazione cartacea

- *l'operatore, per tutto il periodo in cui effettui 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 (vd.distruzione dei documenti cartacei)*
- *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*

Utilizzo dei supporti di memorizzazione

- *è vietato l'utilizzo di supporti rimovibili, come ad esempio floppy disk o cd rom, per lo scambio di dati sensibili; qualora vi fosse assoluta necessità di utilizzarli è indispensabile assicurarsi che essi non vengano riutilizzati e siano distrutti dopo il loro utilizzo; qualora, viceversa, vengano riutilizzati occorre verificare che il precedente contenuto sia stato reso assolutamente irrecuperabile, in quanto le normali procedure di cancellazione di un dato informatico non sono normalmente sufficienti a garantire ciò, potendosi in molti casi recuperare anche dati cancellati con procedure e strumenti particolari .*

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*
- ***la chiamata nominativa dell'utente è vietata**: 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 della prestazione medica delicate (ad es. utilizzo di accorgimenti provvisori, tipo 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.*

Garanzie fornite dall'azienda

L'Azienda definisce quali sono gli uffici e le strutture preposte ai controlli previsti dalla presente linea guida, sarà possibile in qualsiasi momento per l'operatore avere accesso a tali informazioni rivolgendosi a _____.

Facoltà dell'azienda

Qualora l'Azienda:

- abbia ad accertare manomissioni alle configurazioni del sistema informatico, telematico, telefonico aziendale e/o accessi indebiti allo stesso;
- riscontri diffusioni indebite di informazioni atte a pregiudicare la sicurezza del sistema informatico, telematico, telefonico aziendale o il suo buon funzionamento e/o a garantire ad altri accessi o altri privilegi non dovuti;
- abbia concrete ragioni che portino a pensare che la sicurezza del sistema tecnologico aziendale possa essere minacciata

si riserva il diritto di:

c. effettuare controlli specifici tesi ad accertare lo stato dei fatti relativamente all'uso delle attrezzature aziendali;
d. disabilitare le autorizzazioni all'accesso e all'uso delle attrezzature aziendali;
e. segnalare al responsabile organizzativo situazioni e comportamenti anomali degli operatori.

In caso di problemi inerenti la sicurezza della infrastruttura tecnologica l'azienda si riserva il diritto di adottare tutte le misure tecniche che garantiscano la gestione della contingenza, ad esempio isolando dalla rete stazioni che siano state infettate da virus che ne pregiudichino il buon funzionamento, aggiornando configurazioni software e/o hardware, ecc… Tutte le azioni messe in atto dovranno essere valutate in una logica di costo/beneficio e dovranno essere improntate ad un criterio di minimizzazione del disservizio.

L'azienda si riserva la facoltà di sospendere l'accesso ai servizi qualora anche a seguito di segnalazioni rappresentate dal Responsabile Organizzativo sussistano nel tempo reiterate evidenze delle inadempienze da parte dell'operatore.

L'azienda si riserva la possibilità di interrompere i servizi informatici per le manutenzioni ordinarie e straordinarie e per la gestione dei guasti, impegnandosi tuttavia, nel limite del possibile, ad avvertire preventivamente gli utenti di dette interruzioni.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : T0305

Oggetto : Elenco connessioni VPN

Data Ultima Modifica : 23/04/2013

Di seguito l'elenco dei certificati attivati per le connessioni VPN

3T Telecomunicazioni	Stradello Agostini 3, Parma
A. Demori	Via Portaluppi 15, Milano
Ad Personam	Via Cavestro 14, Parma
ADS	Via del Lavoro 17, Bologna
AICOD	Via Cassio Parmense 3, Parma
ASP Azienda Sociale Sud-Est (Val Parma)	Via Don Orsi 1, Langhirano (PR)
ASP Cav. Marco Rossi Sidoli	Via Duca degli Abruzzi 27, Parma
ASP Sede Legale Fidenza	Viale Berenini 151, Fidenza (PR)
Axios Informatica	Via Sebastian Bach 7, Bassano del Grappa (VI)
Azienda USL di Bologna	Via Castiglione 29, Bologna
Azienda USL di Padova	Via Casa di Ricovero 40, Cittadella (PD)
Biomerieux	Via di Campigliano 58, Firenze
Carestream	Via al Porto Antico 6, Genova
Casa Anziani Collecchio	Via Aldo Moro 2, Collecchio (PR)
Casa degli Anziani di Sorbolo	Via Beethoven 11, Sorbolo (PR)
Casa di Cura Città di Parma	Piazzale Maestri 5, Parma
Casa per Anziani Fondazione Cav. B. Patrioli	Via Giuseppe Verdi 37, Medesano (PR)
Casa Protetta Ca' Bonaparte	Località Ca' Bonaparte, Neviano degli Arduini (PR)
Casa Protetta Città di Fidenza	Via Esperanto 13, Fidenza (PR)
Casa Protetta Città di Salsomaggiore	Viale Rimembranze 17, Salsomaggiore (PR)
Casa Protetta Don Gottofredi	Strada Ospedale 4, Roccabianca (PR)
Casa Protetta Don Prandocchi Cavalli	Via Don Minzoni 24, Sissa (PR)
Casa Protetta Gino Cavazzini	Via Olari 6, Berceto (PR)
Casa Protetta Lorenzo Peracchi	Via XXIV Maggio 16, Fontanellato (PR)
Casa Protetta Ospedale Dagnini	Viale Matteotti 23, Zibello (PR)
Casa Protetta P. Corsini	Via Micheli 1, Pellegrino Parmense (PR)
Casa Protetta Pavesi Borsi	Via Matteotti 25, Noceto (PR)
Casa Protetta Pellegrino Parmense	Via Sonnino, Pellegrino Parmense (PR)
Casa Protetta San Mauro	Via Guglielmo Marconi 12, Colorno (PR)
Casa Protetta Santa Rita	Via IV Novembre 32, Soragna (PR)
Casa Protetta Selene Conti	Via Donatori Sangue 4, Borgo val di Taro (PR)
Casa Protetta Tommasina Sbruzzi	Via Battisti 42, San Secondo (PR)
Casa Protetta Villa Pigorini	Via IV Novembre 2, Traversetolo (PR)
Casa Protetta Villa San Bernardo	Strada Bodrio 14, Porporano (PR)
Casa Protetta Zanetti	Via Alla Rocca 1, Varsi (PR)
CEDAS Srl	Via Nazionale 102, Borgo Val di Taro (PR)
Centro di Solidarietà l'Orizzonte	Via Testi 4/a, Parma
Centro Fisioterapico Maria Luigia	Strada della Repubblica 47, Parma
Comune di Fidenza	Piazza Garibaldi 1, Fidenza
Comune di Neviano degli Arduini	Piazza IV Novembre 1, Neviano degli Arduini (PR)
Comune di Trecasali	Via Nazionale 44, Trecasali (PR)
Comune di Zibello	Via Matteotti 10, Zibello (PR)
Comunità di Servizo e Assistenza Betania	Strada del Lazzaretto 26, parma
Comunità Montana Valli Taro e Ceno	Piazza XI Febbraio 7, Borgo Val di Taro (PR)

Comunità Terapeutica Casa di Lodesana	Via Cabriolo 75, Fidenza (PR)
Consorzio Zenit Casa Protetta Alberi di Vigatto	Strada Alberi, Alberi di Vigatto (PR)
Consorzio Zenit Casa Protetta R. Vasini	Via Nazionale, Fornovo (PR)
CSAMED	Via Grado 26, Cremona
Data4	Via Strada della Selva 87, San Bonifacio (VR)
Dedalus	Via Giardini 454/B, Modena
Dialcenter	Via P. Zuffardi 5, Fornovo (PR)
Dialpoint	Via Verdi 24, Traversetolo (PR)
ELCO	Piazza della Vittoria 24/B, Savona
Engineering Sanità Enti Locali	Galleria del Leone 3, Bologna
ET Medical Devices	Via De Zinis 6, Cavareno (TN)
Exprivia	Via Carlo Esterle 9, Milano
Farmacia di Scurano	Via Mercato 141, Scurano (PR)
Farmacia Leonardi	Via Martiri della Libertà 24, Varano de Melegari (PR)
Farmacia Rosso	Via Roma 25, Bore (PR)
Farmacia Scimonelli	Via Roma 18, Varsi (PR)
GPI	Via Ragazzi del '99, Trento
Gruppo Partners Associates	Via Pradamano 30, Udine
IG Consulting	Strada Martinara 325/B, Modena
Info Line Srl	Via Colorno 63/A, Parma
Infocert	Corso Stati Uniti 14, Padova
Instrumentation Laboratory	Viale Monza 338, Milano
KDM	Via Roberto Bracco 42/B, Roma
La Traccia	Recinto Il Fiorentini 10, Matera
ME.TE.DA.	Via Campania 25, San Benedetto del Tronto (AP)
Medical Software System	Via Chiletti 29/2, San Prospero (MO)
Medicina di Gruppo Berceto	Piazza Micheli 8, Berceto (PR)
Medinf	Via Giardini 454/B, Modena
Newteam Srl	Via Chiesa San Cristoforo 1667, Cesena
Nihon Kohden Italia	Via San Tommaso 78, Bergamo
Noemalife	Via Gobetti 52, Bologna
Ospedale Piccole Figlie	Via Po 1, Parma
Partech	Stradello Ada Negri 6, Parma
Poliambulatorio Dalla Rosa Prati	Via Emilia Ovest 12, Parma
PROGEL	Via Due Ponti 2, Argelato (BO)
Rastelli Giovanni (Telecom)	Via Argine 30, Soragna (PR)
Residenza Villa Matilde	Via Bracchi 10, Felino (PR)
SAA Langhirano	Piazza Ferrari 5, Langhirano (PR)
Santa Lucia Ingegneria Biomedica	Via Vittime della Strada 2, Gragnano Tr. (PC)
Sferacarta Net	Via Bazzanese 69, Casalecchio di Reno (BO)
SIOMED	Via Porta Est 17, Venezia
Studio Magdala	Via Crespi 41/A, Bologna
Studio Medico Associato Fidenza	Via Bacchini 18, Fidenza (PR)
Università di Modena e Reggio Emilia	Viale A. Allegri 9, Reggio Emilia
Villa Mater Gratiae	Via Madonnina 233bis, Bardi (PR)
Zen Sistemi	Via Pizzetti 2, Reggio Emilia

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Parma

Nome Documento : P0104

Oggetto : Videosorveglianza

Data Ultima Modifica :20/03/2009

Nel rispetto della direttiva 29 aprile 2004, emanata dal Garante per la privacy in materia di installazione ed utilizzazione di impianti di videosorveglianza, l'Azienda USL ha:

Impianti installati in strutture dell'Azienda USL di Parma sia per il controllo dei pazienti ricoverati che per il controllo degli accessi.

IMPIANTI VIDEOSRVEGLIANZA

STRUTTURA	INDIRIZZO	N° VIDEOCAMERE
Dipartimento di Sanità Pubblica	Via Vasari (PR)	4
Neuropsichiatria Infantile	Via Bocchi/angolo Via Savani (PR)	4
Centro Autismo	Via La Spezia (PR)	4
Polo Sanitario Vilma Preti	Via Verona (PR)	3
Dipartimento Tecnico e delle Tecnologie	Via Spalato, 2 (PR)	5
Sede SPOI – SPDC – Padiglione Braga	Ospedale Maggiore di Parma	15
Sede Punto Bianco/Guardia Medica	Via Abbeveratoia n°14 (PR)	2
SERT	Strada Mercati (PR)	6
Centro Distribuzione Metadone	Via del Taglio (PR)	3
Poliambulatori di Fornovo Taro	Via Solferino – Fornovo Taro	2
Polo Sanitario di Langhirano	Via Roma - Langhirano	7
Ospedale di Vaio	Via Don Tincati, 5 - Fidenza	18
Ospedale di San Secondo P.se	Via M.V.Mazza - San Secondo	6

Ai Responsabili delle Strutture Aziendali sono state impartite specifiche disposizioni in ordine al corretto utilizzo dei sistemi di videosorveglianza. Sono stati altresì apposti presso ogni punto (videocamera) specifici cartelli riportanti l'informativa "MINIMA" costituita dall'indicazione del titolare del trattamento e la finalità che si intende perseguire. Gli stessi sono stati posizionati prima del raggio d'azione delle telecamere e sono visibili in ogni condizione di illuminazione ed informano se le immagini sono solo visionate o anche registrate. Nei locali delle Strutture aziendali è affissa l'informativa completa, così come prevista dal citato art. 13 del Codice: E' facilmente accessibile agli interessati e contiene il nominativo di un incaricato perchè la fornisca anche (se richiesto) oralmente.

Letto, confermato, firmato:

IL DIRETTORE AMMINISTRATIVO
Dott. ssa Elena Saccenti

IL DIRETTORE SANITARIO
Dr. Ettore Brianti

IL DIRETTORE GENERALE
Dr. Massimo Fabi

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto certifica che la deliberazione è stata **affissa all'albo** di questa Azienda Unità Sanitaria Locale **IL GIORNO 29/04/2013** e vi rimarrà in pubblicazione per 15 giorni consecutivi ai sensi e per gli effetti del 5° comma dell'art.37 della L.R.20/12/94 n.50 così come modificato dall'art.12 della L.R.23/12/04 n.29.

La presente deliberazione diventa esecutiva dal primo giorno di pubblicazione, come previsto dalla Legge Regionale sopra indicata.

Lì 29/04/2013 IL DIRETTORE AMMINISTRATIVO

Dott.ssa Elena Saccenti

Per copia conforme all'originale ad uso amministrativo.

IL DIRETTORE AMMINISTRATIVO

Dott.ssa Elena Saccenti

La presente deliberazione pubblicata il _____,**soggetta a controllo** della Giunta Regionale
(Legge 30/12/1991 n. 412 Art. 4 c.8)
Data ricevimento Regione prot. n. _____ del _____
Chiarimenti Regione prot n.. _____ del _____
Richiesta chiarimenti ai servizi/uffici prot. n. _____/_____ del _____
Controdeduzioni Regione _____
Regione annullamento parziale/totale prot. _____ del _____
È divenuta esecutiva in data _____
è stata approvata nella seduta della Giunta Regionale del _____

La presente deliberazione viene trasmessa
· al Collegio Sindacale, ai sensi dell'art. 40, comma 3), della Legge Regionale 20 dicembre 1994, n. 50 il 29/04/2013
· al Consiglio dei Sanitari il
· alla Conferenza dei Sindaci il

ai seguenti uffici/servizi: