



Azienda Unità Sanitaria Locale
Piacenza

Azienda Unità Sanitaria Locale Piacenza

D ocumento P rogrammatico della S icurezza

Redatto ai sensi del Decreto legislativo 30 Giugno 2003 n. **196**
“Codice in materia di protezione dei dati personali”

Data

Revisione

Febbraio 2005	02
Aprile 2005	03
Il Titolare del trattamento dei dati personali Azienda USL di Piacenza	

INDICE

1.	INTRODUZIONE	4
1.1	Oggetto e scopo del documento.....	4
1.2	L'AUSL di Piacenza.....	4
1.3	Missione aziendale.....	5
1.4	Unità di trattamento.....	5
1.4.1	Area Ospedaliera.....	5
1.4.2	Area territoriale.....	6
1.4.3	Area di supporto.....	6
2.	IL SISTEMA INFORMATIVO	6
2.1	Categoria e natura dei dati trattati.....	6
2.2	Soggetti cui si riferiscono i dati.....	7
2.3	Finalità dei trattamenti.....	8
2.4	Modalità e strumenti di trattamento.....	8
2.5	Dati oggetto di notifica al Garante.....	8
3.	RUOLI E RESPONSABILITA'	11
3.1	Struttura organizzativa.....	11
3.2	Titolare.....	11
3.3	Responsabili.....	12
3.3.1	Responsabilità della sicurezza logica.....	12
3.4	Incaricati.....	13
4.	IL SISTEMA INFORMATICO	13
4.1.1	Caratteristiche generali.....	18
4.2	Architettura fisica.....	18
4.2.1	Postazioni di lavoro.....	18
	PC PORTATILI.....	18
4.3	DB e file system.....	18
4.4	Trattamenti automatici.....	22
4.4.1	Applicativi sanitari di gestione ospedaliera.....	22
	PRONTO SOCCORSO (PS).....	22
	HOSPITAL 2000.....	22
	ESITO DI ANALISI CLINICHE.....	22
	INFOCLIN.....	22
	MED'S OFFICE : AGENDA DI REPARTO.....	23
	PRENOTAZIONE E ACCETTAZIONE : CUP.....	23
	MEDICINA DI BASE.....	23
	ANAGRAFICA ASSISTITI.....	23
	ADI.....	23
	COMUNICAZIONI CON L'ESTERNO.....	23
4.5	Trattamenti non automatici.....	28
4.5.1	Trattamenti cartacei.....	28
4.5.2	Trattamenti tramite telefono o radio.....	29
4.5.3	Comunicazioni verbali.....	29
5.	GESTIONE COLLABORATORI ESTERNI	29
5.1	Lettera ai fornitori.....	30
6.	ANALISI DEI RISCHI	30
6.1	Rischi che incombono sui dati.....	31
6.1.2	Rischi ambientali.....	31
6.1.3	Integrità dei dati.....	31
	RISCHI DI NATURA ACCIDENTALE.....	31
	RISCHI DA PROGRAMMI DI CUI ALL'ART. 615 QUINQUIES DEL C.P.....	32
	RISCHI DI CARATTERE VOLONTARIO.....	32
6.1.4	Riservatezza dei dati.....	33
	RISCHI DI ACCESSI FRAUDOLENTI DALL'INTERNO.....	33

	RISCHI DI ACCESSI FRAUDOLENTI DALL'ESTERNO	34
	RISCHI DERIVANTI DA TRATTAMENTI NON CONSENTITI O NON CONFORMI ALLE FINALITÀ DELLA RACCOLTA	34
6.1.5	Disponibilità dei dati.....	34
	RISCHI DI CARATTERE ACCIDENTALE	35
	RISCHI DI CARATTERE INTENZIONALE.....	35
6.1.6	Ulteriori rischi di cui all'art.615 ter del codice penale.....	35
6.2	Riepilogo dell'analisi dei rischi.....	37
6.3	Misure in essere	44
6.3.1	Sicurezza fisica.....	44
	SERVER FARM	44
	DOCUMENTAZIONE CARTACEA	44
6.3.2	Sicurezza logica	44
	SICUREZZA PERIMETRALE	44
	SISTEMA DI AUTENTICAZIONE E AUTORIZZAZIONE.....	44
	POLITICHE DI BACKUP	45
	ANTIVIRUS	45
	PROTEZIONE DELLA SESSIONE DI LAVORO	46
	RIUTILIZZO CONTROLLATO DEI SUPPORTI IN AMBIENTE PC	46
6.3.3	Sicurezza organizzativa.....	46
6.4	Misure da adottare.....	46
6.4.1	Introduzione della Smart Card.....	46
6.4.2	Sicurezza fisica.....	47
6.4.3	Revisione del sistema di autenticazione/autorizzazione	47
6.4.4	Revisione delle politiche di back-up	47
6.4.5	Evoluzione del sistema di refertazione	47
6.5	Piano delle attività	47
7.	FORMAZIONE / INFORMAZIONE	48
7.1	Attività già effettuate	48
7.2	Attività previste	48
7.2.1	Formazione di base	48
7.2.2	Formazione specifica.....	48
7.2.3	Informativa capillare	48
7.2.4	Pubblicazione sulla intranet.....	49
8.	ELENCO ALLEGATI	49

1. INTRODUZIONE

1.1 Oggetto e scopo del documento

L'obiettivo del DPS è quello di fornire uno strumento per documentare e verificare la corretta ed efficace applicazione delle misure minime di protezione dei dati personali e sensibili e del loro trattamento, nell'ambito delle attività svolte dall'Azienda, in ottemperanza ai requisiti dell'Allegato B del Codice.

L'Azienda, consapevole che la sicurezza del sistema informativo non dipende soltanto da aspetti tecnici, ma anche, se non principalmente, da quelli organizzativi, sociali e legali, coglie l'occasione dell'adempimento imposto dal D.Lgs. 196/2003, per rielaborare un documento programmatico sulla sicurezza come utile strumento per:

- formalizzare, razionalizzare e finalizzare le strategie aziendali in materia di sicurezza;
- definire opportune strategie per l'informazione e la formazione degli utenti aziendali sugli aspetti di sicurezza.

1.2 L'AUSL di Piacenza

L'AUSL di Piacenza, per i propri fini istituzionali, gestisce dati personali e sensibili per i quali deve redigere un Documento Programmatico della Sicurezza (DPS). L'Azienda ha competenza sull'intero territorio provinciale, nel quale si trovano 4 ospedali.

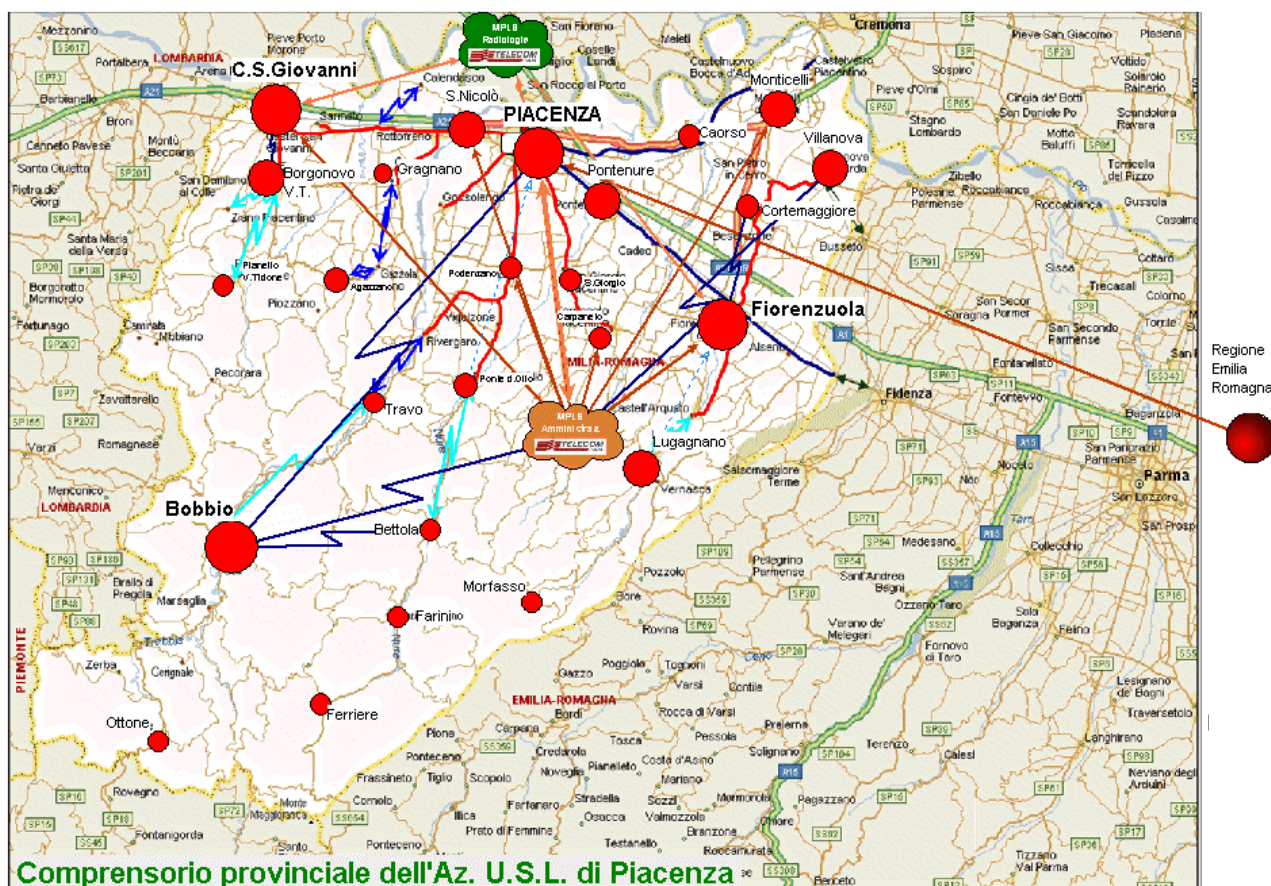


Fig. 1 Territorio della Provincia di Piacenza

1.3 Missione aziendale

L'AUSL di Piacenza, per i propri fini istituzionali, gestisce dati personali e sensibili per i quali, entro il 31 Marzo 2005, deve redigere un Documento Programmatico della Sicurezza (DPS) che verrà indicato nella relazione accompagnatoria al bilancio.

L'Azienda ha competenza sull'intero territorio provinciale, nel quale si trovano 4 ospedali.

La *Missione Aziendale* si propone:

- La tutela della salute come diritto di Cittadinanza.
- La presa in carico dei bisogni di salute del cittadino, espressi sia in forma individuale che in forma collettiva.
- L'attuazione di interventi di prevenzione, di promozione della salute, di cura e riabilitazione della persona.
- La garanzia dei livelli essenziali di assistenza, consolidando l'integrazione tra l'assistenza territoriale e quella ospedaliera.
- La garanzia di utilizzo corretto delle risorse, anche da un punto di vista economico.

L'Azienda UsI di Piacenza si è costituita il 1° luglio 1994. E' nata dalla fusione di tre Unità Sanitarie Locali ed estende la sua competenza su tutto il territorio della Provincia di Piacenza.

- Popolazione residente al 31/12/2000: 267.164
- Superficie territoriale (kmq): 2.589,46
- Densità demografica (abitanti /kmq): 103,17
- Comuni della provincia: 48
- N° Distretti: 4
- N° Presidi Ospedalieri (7 stabilimenti ospedalieri pubblici): 4
- N° Dipendenti (forza complessiva occupata al 31/12/2000): 3451
- N° posti letto previsti nel PAL per acuti: 882

di cui:

- posti letto per day -hospital **107**
- posti letto "tecnici" di dialisi **36**
- posti letto di lungo-degenza **163**

1.4 Unità di trattamento

Le unità di trattamento sono tre.

1.4.1 Area Ospedaliera

L'unità di trattamento Area Ospedaliera è organizzata nei seguenti Dipartimenti:

- Funzioni radiologiche;
- Non autosufficienza e riabilitazione;
- Chirurgia generale;
- Chirurgia specialistica/ortopedica;
- Onco-ematologia
- Medicina specialistica;
- Medicina generale;
- Patologia clinica;
- Emergenza/Urgenza.
- Maternità/Infanzia/Età evolutiva;
- Presidio unico ospedaliero;

- Farmaceutico

Tali dipartimenti erogano i loro prodotti di specialistica ambulatoriale e strumentale, ricovero, day hospital, consulenza, trattamenti riabilitativi, emergenza/urgenza, screening, interventi educativi.

1.4.2 Area territoriale

L'area territoriale è organizzata nel seguente modo:

- Distretto di Piacenza
- Distretto della Montagna
- Distretto della Val Tidone
- Distretto della Val D'arda
- Dipartimento Cure primarie
- Dipartimento di Sanità Pubblica
- Dipartimento di Salute Mentale

1.4.3 Area di supporto

L'unità di trattamento dell'area di supporto è composta da :

- Dipartimento Amministrativo
- Dipartimento degli staff

2. IL SISTEMA INFORMATIVO

Da un punto di vista assolutamente generale le attività istituzionali di una AUSL si possono dividere in Amministrative e Sanitarie. Ambedue comportano flussi informativi interni ed esterni all'Azienda e coinvolgono collaboratori che possono essere o meno alle dirette dipendenze della AUSL.

Le modalità con cui i dati personali e sensibili sono trattati possono essere le più disparate e prevedono sia sistemi di elaborazione automatica che utilizzi di tipo cartaceo (documenti autografi, stampe di documenti elettronici, modulistica, fax, fotocopie, etc) o verbale (radio, conversazioni, lezioni, etc).

In questo paragrafo viene data una panoramica delle informazioni trattate, con particolare attenzione a quelle che sono state oggetto di notifica al Garante

2.1 Categoria e natura dei dati trattati

- **INFORMAZIONI ANAGRAFICHE** : elementi d'identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato e di lavoro, Codice Fiscale, num. di libretto sanitario, num. di telefono, di telefax, indirizzo di posta elettronica, numero carta d'identità, passaporto, patente di guida, n. posizione previdenziale e assistenziale, targa automobilistica, dati fisici quali altezza e peso);
- **STATO DI SALUTE** questo tipo di informazione è relativa sia agli assistiti che al personale dipendente (certificati medici per assenza a causa di malattie). In particolare i dati sanitari riguardano : diagnosi, prognosi, cure, prestazioni, referti, interventi, analisi, analisi strumentali.
- **DATI GENETICI** in carico al centro trasfusionale, ematologia, nefrologia, procreazione assistita
- **DATI RELATIVI ALLA FAMIGLIA** e a situazioni personali (stato civile, minori a carico, consanguinei, altri appartenenti al nucleo familiare);

- **ISTRUZIONI E CULTURA** (pianificazione degli iter formativi interni, curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audio-visivo, ecc. - titoli di studio);
- **LAVORO** Queste informazioni sono relative prevalentemente ai dipendenti e riguardano : occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione personale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae o lavorativo, competenze professionali, retribuzione, assegni, integrazioni salariali e trattenute, beni aziendali in possesso del dipendente;
- **ADESIONE A SINDACATI** od organizzazioni a carattere sindacale; relativi a dipendenti iscritti a sindacati cui l'azienda versa la quota associativa.
- **CONVINZIONI RELIGIOSE**, adesioni ad organizzazioni a carattere religioso; (assistenza religiosa ai ricoverati, diete alimentari derivanti da particolari pratiche e convinzioni religiose,....)
- **DATI CONTABILI**, ordini, buoni di spedizione, fatture, articoli, prodotti, servizi, contratti, accordi, transazioni, identificativi finanziari, solvibilità, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi, dati assicurativi, dati previdenziali);
- Informazioni di tipo **GIUDIZIARIO** (sulla posizione nel casellario giudiziale richieste ai dipendenti all'atto dell'assunzione, contenziosi sia penali che civili con soggetti interni ed esterni all'Azienda).
- Dati sul **COMPORAMENTO** (valutazione dei comportamenti dei pazienti oggetto di cure psicologiche e/o psichiatriche e di pazienti affetti da dipendenze da droghe)
- Dalla AUSL di Piacenza dipende anche il 118, dotato di strumenti di **GEOREFERENZIAZIONE (GIS) DEI MEZZI SANITARI** che intervengono a fronte delle chiamate. Lo stesso sistema acquisisce informazioni sull'esatta ubicazione geografica del sito su cui è necessario inviare le ambulanze e il personale medico o paramedico.

2.2 Soggetti cui si riferiscono i dati

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

- **CITTADINO UTENTE** delle prestazioni sanitarie (vengono fornite prestazioni a tutti i cittadini italiani e stranieri che si presentino presso gli ospedali della AUSL). In particolare esiste una anagrafica di tutti i residenti della provincia di Piacenza in possesso di libretto sanitario
- **PERSONALE DIPENDENTE**;
- **PERSONALE NON DIPENDENTE** (retribuito o meno) che collabora con l'Amministrazione o con società, enti, associazioni, etc che offrono prestazioni all'AUSL:
 - **LAVORATORI AUTONOMI e LIBERI PROFESSIONISTI**
 - **MEDICI VOLONTARI**
 - **STUDENTI** delle 2 scuole interne all'Azienda (esistono corsi per "fisiocinesiterapisti" e per "infermieri professionali")
 - **CONSULENTI**;
 - **SPECIALIZZANDI**
 - **BADANTI**
 - **ADERENTI AD ASSOCIAZIONI POLITICHE, RELIGIOSE O SINDACALI**;
- **SOGGETTI OD ORGANISMI PUBBLICI**;
- **CANDIDATI** da considerare per l'instaurazione di un rapporto di lavoro;
- **FREQUENTATORI**
- **FAMILIARI E AFFINI** dell'interessato.

2.3 Finalità dei trattamenti

Le finalità del trattamento¹ sono riconducibili alle seguenti macro-categorie :

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

2.4 Modalità e strumenti di trattamento

Le informazioni personali e sanitarie vengono trattate in modalità diversificate :

- Con "strumenti elettronici"²
- Con l'ausilio di supporti cartacei (cartelle cliniche, prescrizioni, richieste di analisi cliniche, referti, comunicazioni tra reparti, fax, etc.)
- Via radio e telefono (comunicazioni col 118, comunicazioni con le autoambulanze in servizio, comunicazioni tra i vari reparti e ospedali, etc.)
- Verbali (comunicazioni con i pazienti, i parenti, il personale addetto,)

2.5 Dati oggetto di notifica al Garante

In particolare l'Amministrazione ha inviato notifica al Garante per il trattamento di **DATI GENETICI** e per quelli **IDONEI A RIVELARE LO STATO DI SALUTE E LA VITA SESSUALE**, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffuse, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria.

La tabella della pagina seguente riassume informazioni relative a questa tipologia di dati e contenute nella notifica.

¹ **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;

² "**Strumenti elettronici**", sono "gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Tipologia dei dati	Soggetti cui si riferiscono i dati	Finalità del trattamento	Modalità di trattamento
DATI GENETICI			
<ul style="list-style-type: none"> • Dati idonei a rilevare patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali. • Dati idonei a rilevare la gravità o il decorso del quadro clinico delle patologie genetiche. • Dati idonei a identificare malattie ereditarie. • Dati relativi alle malformazioni congenite la cui causa non è nota. • Dati idonei ad accertare maternità o paternità. • Dati relativi a trapianti di tessuti od organi o all'impiego di cellule staminali. • Dati relativi alla procreazione • Dati tratti da studi di relazione tra patrimonio genetico e fattori di rischio. 	<ul style="list-style-type: none"> • Concepiti e nati • Coniugi e conviventi • Persone disabili • Genitori • Parenti, affini o conviventi 	<ul style="list-style-type: none"> • Prevenzione di determinate patologie. • Cura e terapia degli interessati • Cura e terapia dei familiari dell'interessato • Cura e terapia di terzi • Programmi terapeutici o di prevenzione • Diagnosi delle patologie genetiche (test diagnostici) • Diagnosi di patologie descritte nel registro nazionale delle malattie rare • Diagnosi prenatali • Prevenzione di patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali • Ricerca medica o biomedica. • Ricerca statistica • Trapianti di organi e tessuti 	<ul style="list-style-type: none"> • Organizzazione in banche dati in forma prevalentemente automatizzata • Raccolta di dati presso l'interessato. • Raccolta di dati presso terzi. • Indagini per valutare la suscettibilità a patologie genetiche (test di suscettibilità o predittivi)

Tipologia dei dati	Soggetti cui si riferiscono i dati	Finalità del trattamento	Modalità di trattamento
DATI IDONEI A RIVELARE LO STATO DI SALUTE E LA VITA SESSUALE, TRATTATI A FINI DI PROCREAZIONE ASSISTITA			
<ul style="list-style-type: none"> • Dati idonei a rivelare l'identità del donatore • Dati idonei a rivelare l'identità del ricevente • Dati idonei a rivelare la vita sessuale • Dati idonei a rivelare lo stato di disabilità • Dati idonei a rivelare sieropositività • Dati idonei a rivelare malattie infettive e diffuse • Dati idonei a rivelare malattie mentali • Dati idonei a rivelare stato di salute • Dati relativi a indagini epidemiologiche • Dati relativi a prescrizioni farmaceutiche e cliniche • Dati relativi ad esiti diagnostici e programmi terapeutici • Dati relativi all'utilizzo di particolari ausili protesici • Dati relativi alla prenotazione di esami clinici e visite specialistiche • Dati idonei a rivelare AIDS conclamato 	<ul style="list-style-type: none"> • Assistiti • Concepiti e nati • Deceduti • Donatori o riceventi • Genitori • Gruppi familiari • Gruppi omogenei per provenienza geografica • Lavoratori o collaboratori • Maggiori di età • Malati gravi o sottoposti a particolari trattamenti di cura • Minori di età • Neonati (entro il primo anno di vita) • Parenti, affini o conviventi • Pazienti • Personale dipendente • Scolari o studenti di ogni ordine e grado • Soggetti con limitata capacità di intendere e volere • Gruppi omogenei per altre caratteristiche 	<ul style="list-style-type: none"> • Assistenza sanitaria • Trapianto di organi e tessuti • Attività di teleconsulto, telediagnosi o telemedicina • Diagnosi, cura o terapia dei pazienti • Gestione amministrativa • indagine epidemiologica • interventi in caso di calamità, epidemie o malattie infettive • monitoraggio della spesa sanitaria • Prevenzione di patologie genetiche in popolazioni a rischio • Prenotazione e refertazione di esami clinici o visite specialistiche per via telematica o telefonica • Prescrizione elettronica dei farmaci • Procreazione assistita • Registrazione dei pazienti • Ricerca medica o biomedica • Rilevazione di malattie infettive e diffuse • Rilevazione di malattie mentali • Rilevazione di stati di sieropositività • Schede cliniche informatizzate • Sperimentazione clinica • Screening sulla popolazione 	<ul style="list-style-type: none"> • Organizzazione in banche dati in forma prevalentemente automatizzata • Raccolta di dati presso l'interessato. • Raccolta di dati presso terzi • Indagini per valutare la suscettibilità a patologie genetiche (test di suscettibilità o predittivi)

3. RUOLI E RESPONSABILITA'

3.1 Struttura organizzativa

L'attuale organizzazione aziendale è definita dalla delibera n° 342 del 16 Luglio 2004, secondo la quale sono previsti

- Dipartimenti
- Unità Organizzative complesse
- Unità Organizzative semplici dipartimentali
- Distretti

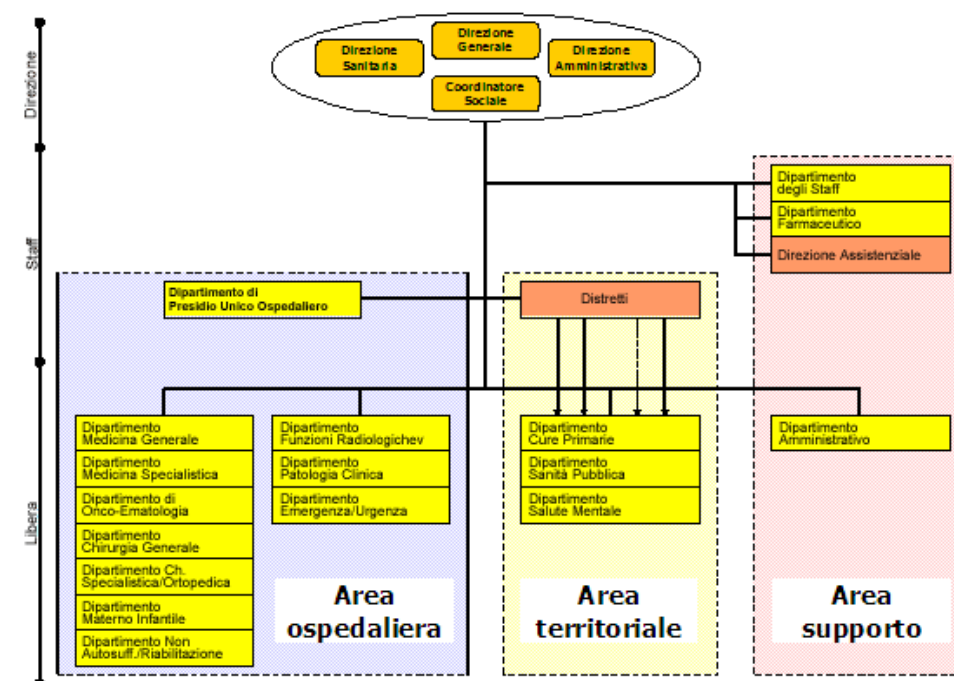


Fig. 2 Le Unità Organizzative

3.2 Titolare

Ai sensi dell'art. 4, comma 1, lettera f) del Codice, il titolare del trattamento dei dati personali è 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.

Titolare del trattamento dei dati personali è l' AZIENDA SANITARIA LOCALE DELLA PROVINCIA DI PIACENZA (nel seguito anche Azienda), con sede legale in Corso Vittorio Emanuele 2°, 149 nella persona del Direttore Generale Francesco Ripa di Meana.

Il Titolare del trattamento dei dati personali:

1. approva il DPS;
2. riferisce, nella relazione accompagnatoria del bilancio d'esercizio, l'avvenuta redazione o aggiornamento del DPS (regola 26);
3. nomina il Responsabile o i Responsabili del trattamento nei termini richiesti dall'art. 29 del Codice.

3.3 Responsabili

Per effetto dell'articolo 29 del Codice:

1. il Responsabile è designato dal titolare facoltativamente;
2. se designato, il Responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
3. ove necessario, per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti;
4. i compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare;
5. il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle proprie istruzioni.

L'elenco dei Responsabili è stato individuato in base a un criterio che tenesse conto delle specifiche competenze e del livello di delega necessario a imporre le scelte strategiche in materia di privacy e sicurezza dei dati e delle informazioni personali e sensibili.

Tali nomine sono state poste in relazione ai compiti e alle funzioni di ciascun Responsabile in maniera da poter raggruppare per classi omogenee di comportamento analoghi, profili di autorizzazioni al trattamento correlati alle disposizioni aziendali già in essere e stabiliti dai regolamenti interni e rapportati ai profili di autorizzazione per l'accesso ai sistemi informatici.

L'elenco completo dei Responsabili individuati e copia dell'atto formale con cui sono stati nominati è reperibile presso l'Unità Operativa Affari Generali e Legali (Dott.ssa Fogliazza).

3.3.1 Responsabilità della sicurezza logica

Il Responsabile, ai fini del DL 196, della sicurezza dei dati e delle informazioni trattate elettronicamente è il dirigente dell'Unità Operativa Sistemi Informativi (UOSI) dott. Flavio Bisotti. Tra i compiti dell'UOSI sono compresi :

- Provvedere, in accordo con i proprietari dei dati e delle applicazioni e con la direzione aziendale, a definire le regole di accesso ai dati e la loro classificazione dal punto di vista della sicurezza.
- Provvedere a dotare l'Azienda degli strumenti tecnici necessari all'applicazione delle regole definite.
- Predisporre, in accordo con i dirigenti delle UOA le regole per la gestione dei profili di accesso ai dati.
- Verificare che le strutture sistemiche garantiscano la separazione degli ambienti e dei ruoli.

Di seguito viene data una breve descrizione dell'organizzazione di questa UO.

Il gruppo di lavoro è costituito da 11 dipendenti dell'Azienda (1 dirigente e 10 operativi).

Per motivi di efficienza e intercambiabilità per ogni funzione "critica" sono previste almeno due persone in grado di svolgere/gestire tutte le attività ad essa connesse. Le singole persone hanno più di una competenza specifica e sono in grado di svolgere più ruoli all'interno del gruppo, a seconda delle necessità contingenti.

In particolare :

- **3 AMMINISTRATORI DI DOMINIO** : hanno un profilo d'accesso logico con caratteristiche di "amministrazione" che consente loro di operare con i pieni diritti sulle informazioni gestite elettronicamente. Esiste inoltre la possibilità di impostare una password "*Administrator Equivalent*" valida nei soli giorni festivi e nel pomeriggio dei prefestivi, assegnata ai membri del gruppo di turno. Questa password è ovviamente temporanea e viene modificata ogni volta.

- **2 AMMINISTRATORI DEGLI APPARATI DI RETE**, responsabili della loro configurazione, che operano solo previo utilizzo di password personale. Inoltre sugli apparati critici esistono "access list" basate sull'indirizzo IP
- **2 ESPERTI DI APPLICATIVI**
- **2 ESPERTI DI BASI DATI**
- **1 COORDINATORE**

A supporto del gruppo interno sono stabilmente impiegate **5 RISORSE ESTERNE**, tutte della ditta EuroSoft che fornisce gli applicativi sanitari. Questo personale si occupa essenzialmente di fornire supporto per la manutenzione evolutiva e l'installazione e configurazione dei propri prodotti. Per la manutenzione e assistenza agli apparati esiste un contratto di outsourcing con la società "Emilia Informatica", che, nell'ambito di questa attività fornisce anche 2 tecnici che fungono da help desk di primo livello.

A questi collaboratori esterni, come a tutti gli altri che, a qualsiasi titolo, forniscono prodotti o servizi di ogni genere all'Amministrazione, è fatto obbligo di rispettare gli stessi comportamenti cui sono tenuti i dipendenti in tema di riservatezza delle informazioni personali e sensibili di cui venissero a conoscenza nello svolgimento del loro lavoro.

3.4 Incaricati

Per il tipo di attività svolta dall'Azienda USL di Piacenza e per le modalità con cui i dati personali e sensibili possono essere trattati (si veda § 3.4 del presente documento), qualsiasi dipendente può, a rigor di norma, essere configurato come "incaricato".³

Per questo motivo l'Azienda ha deciso di raggiungere tutti i dipendenti con una comunicazione con cui li si rende noto dei loro obblighi in materia di riservatezza e sicurezza delle informazioni personali e sensibili.

L'informativa verrà comunicata capillarmente tramite un piano di informazione pianificato per il secondo semestre di quest'anno.

Gli incaricati che svolgono operazioni di trattamento di dati particolari utilizzando elaboratori connessi in rete sono autorizzati all'accesso agli strumenti ed alle operazioni di trattamento, attenendosi alle norme di sicurezza stabilite dall'Azienda per tali trattamenti e per tali modalità di trattamento.

Si è deciso di raggruppare gli incaricati in classi omogenee, così come riportato nella delibera appositamente redatta.

4. IL SISTEMA INFORMATICO

Qui di seguito si riporta la locazione fisica e logica dei sistemi che compongono il sistema informatico:

³ "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

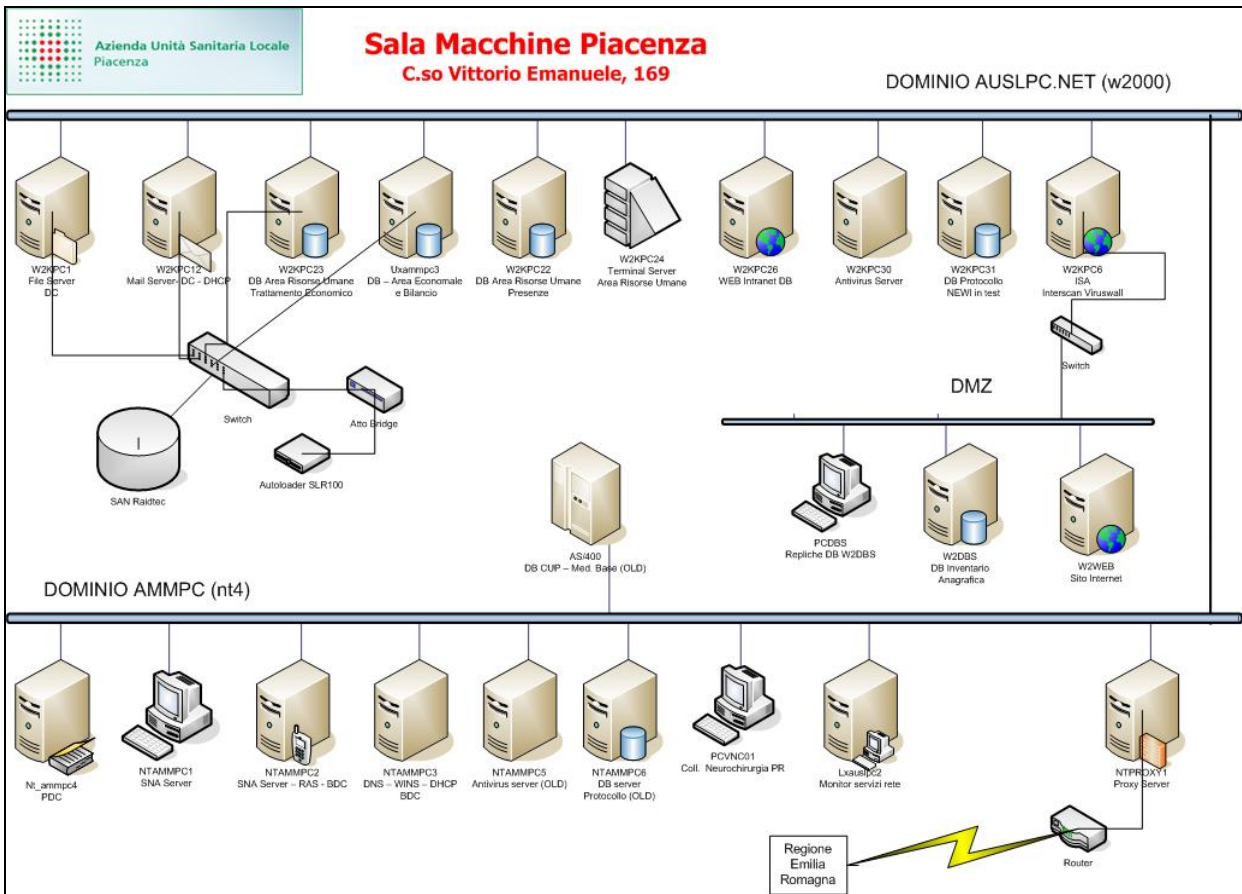


Fig. 5 CED Piacenza Corso Vittorio Emanuele

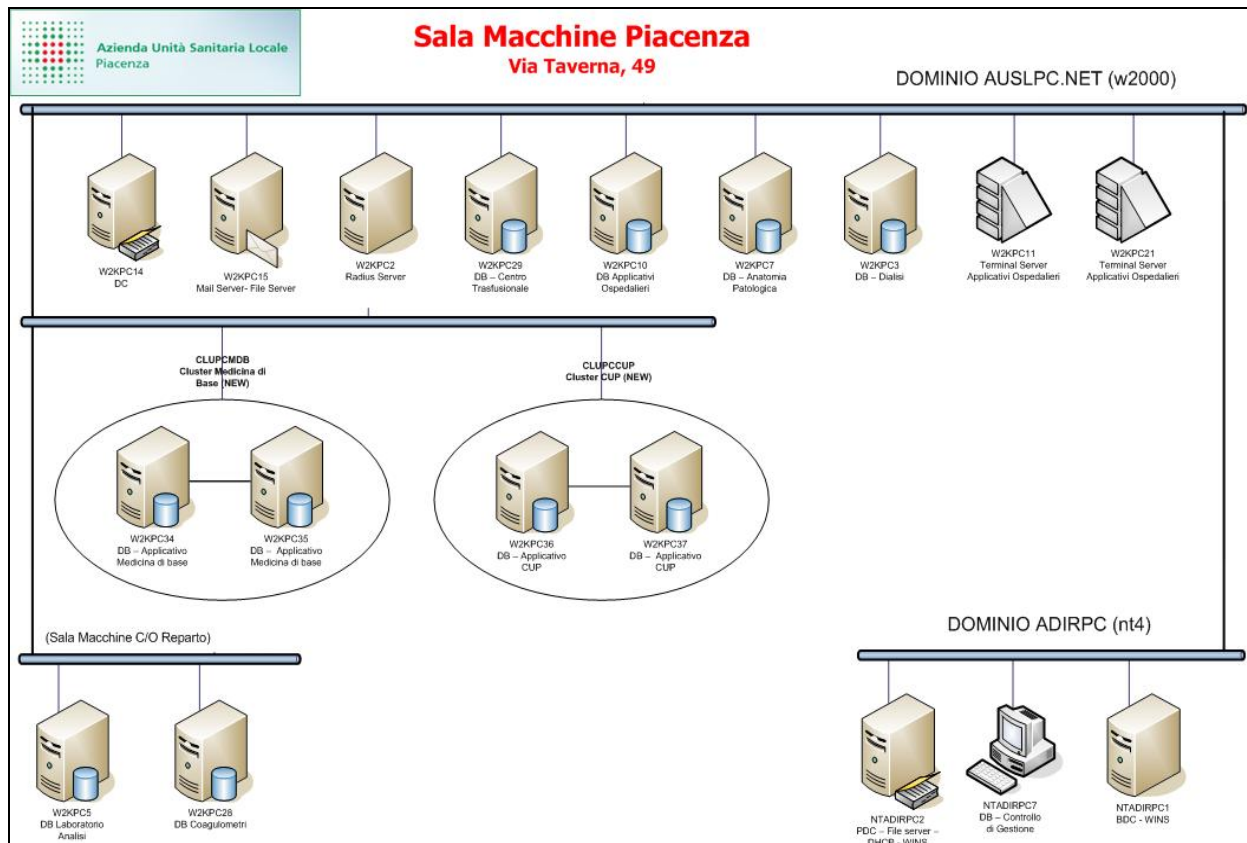


Fig. 6 CED Piacenza Via Taverna

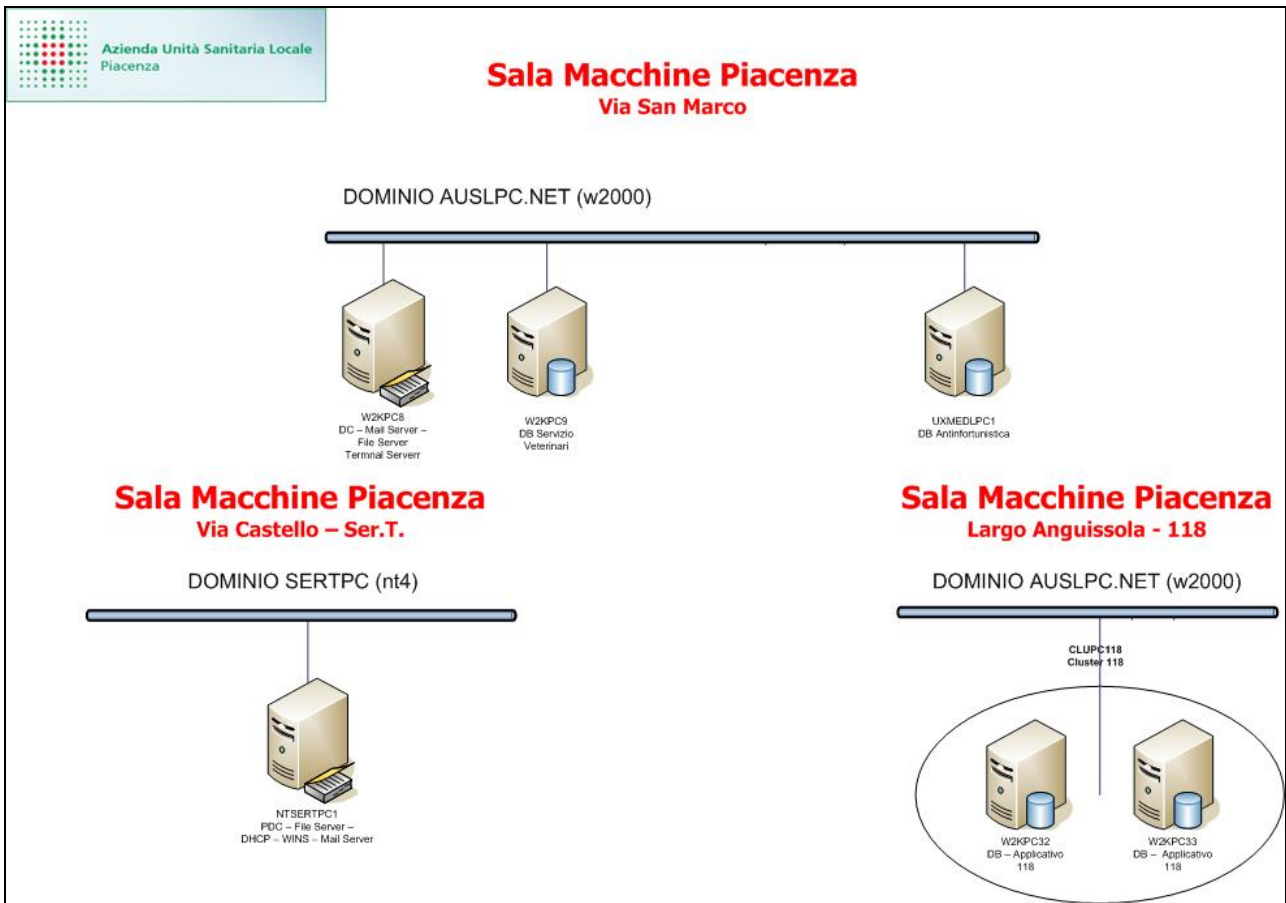


Fig. 7 CED Piacenza Via S. Marco

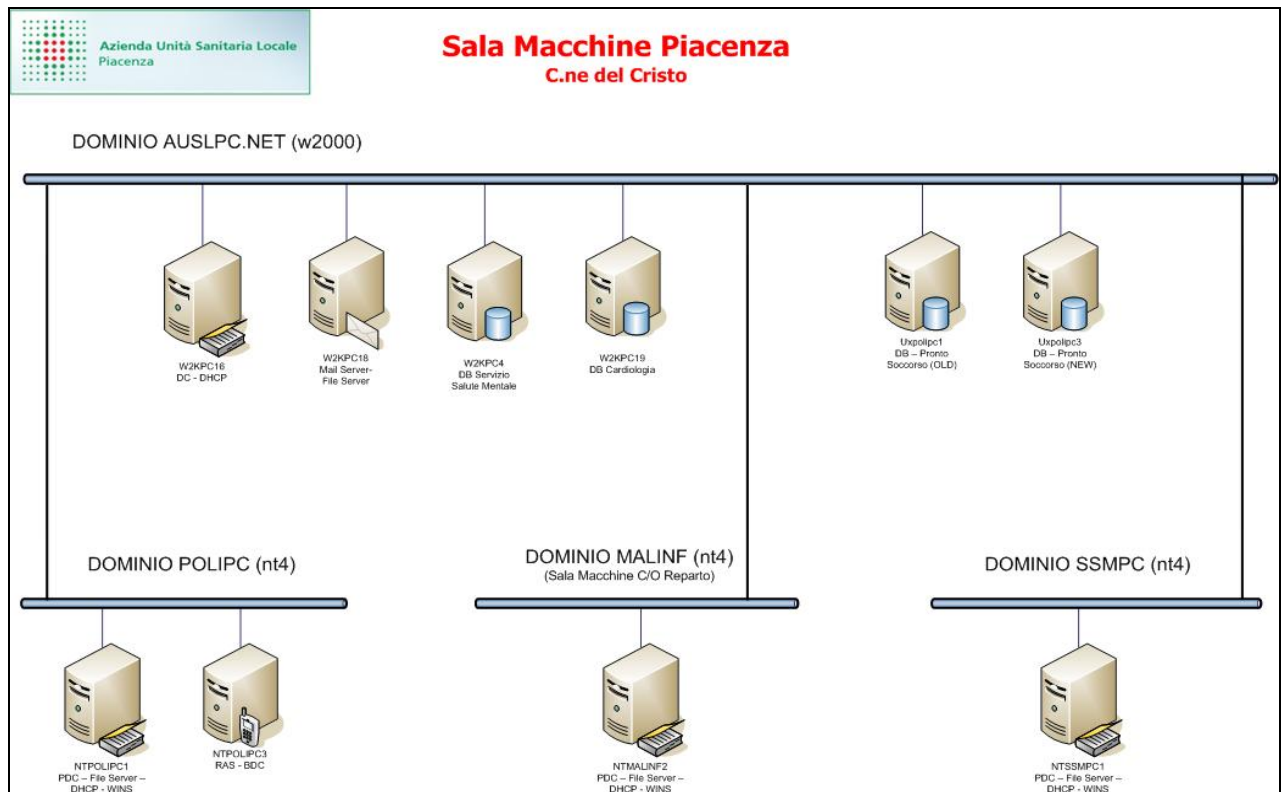


Fig. 8 CED Piacenza Cantone del Cristo

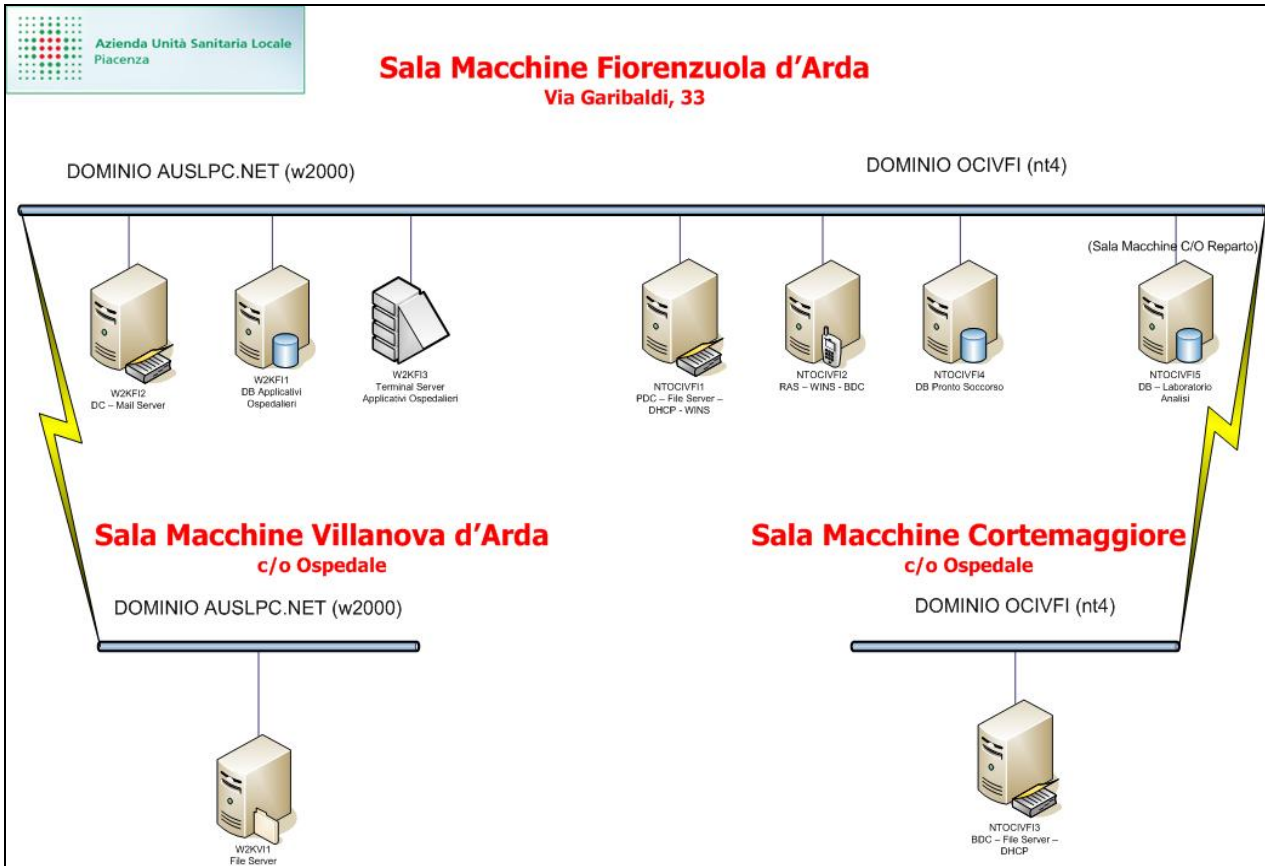


Fig. 9 CED Fiorenzuola d'Arda

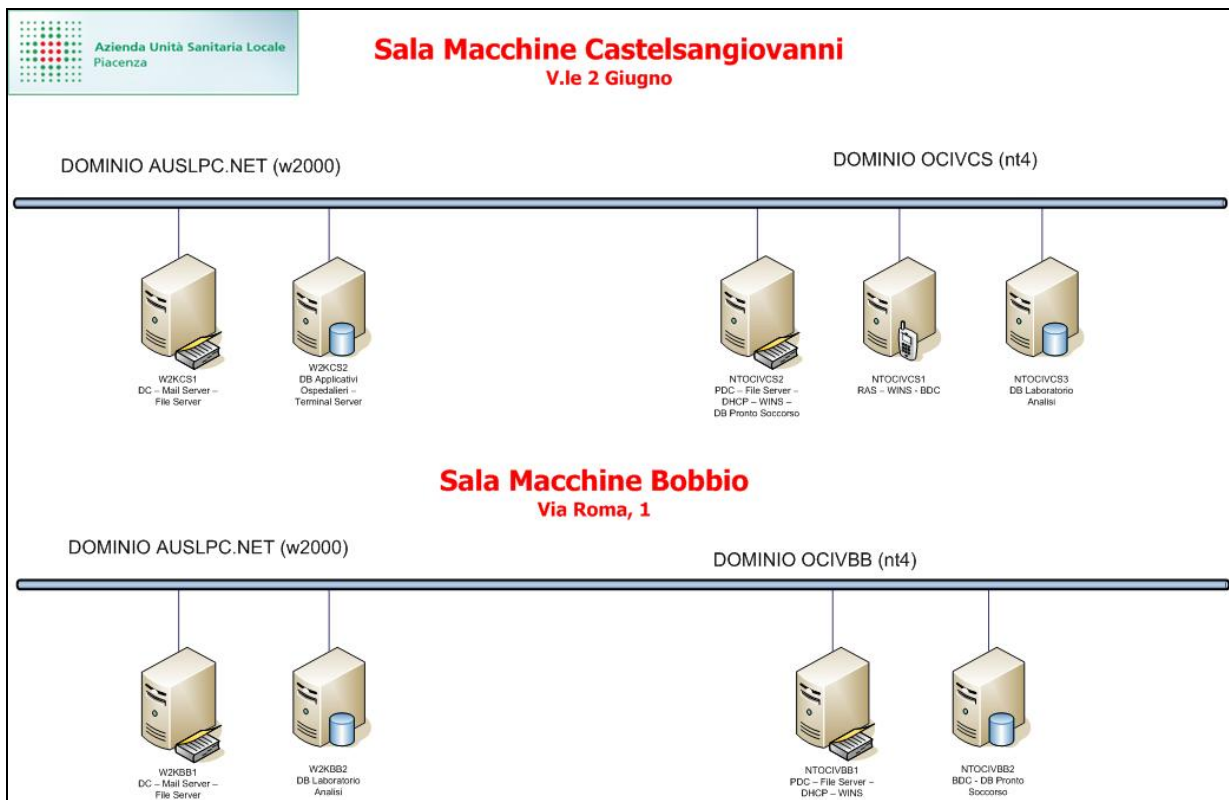


Fig. 10 CED Castesangiovanni e Bobbio

4.1.1 Caratteristiche generali

La progettazione dell'intera architettura dei sistemi informativi di Piacenza ha seguito le linee guida attuali per la realizzazione di centri servizi. In tutte le sale CED, in cui ne esista la necessità, sono state realizzate suddivisioni in reti e sottoreti che implementano principi di "segregation of duties". Sono utilizzate di coppie di firewall installati in modalità HA. Nelle sale macchine che hanno funzioni di accesso dall'esterno (portale per i cittadini, portale intranet per i dipendenti) sono presenti le reti DMZ per separare i servizi pubblici, quali i web server, da quelli interni di back-end.

E' stata realizzata una struttura per il back-up/restore dei dati. I dettagli delle politiche vengono riportati nel relativo paragrafo.

Le macchine che ospitano DB critici sono installate in configurazione HA cluster (118, CUP e Medicina di base).

4.2 Architettura fisica

L'UOSI ha provveduto a redigere un'accurata descrizione del sistema informatico in termini di dislocazione fisica degli apparati e di tipologia e modalità di collegamenti presso le diverse sedi

4.2.1 Postazioni di lavoro

Nessun utente di una postazione di lavoro (persona o gruppo) ha le abilitazioni di amministratore. Sui dispositivi messi a disposizione dall'azienda non è possibile installare nuovi sw senza l'intervento e l'autorizzazione dello UOSI

Esiste una specifica policy aziendale che proibisce l'utilizzo di strumenti personali per collegarsi alla rete interna della USL.

Viene periodicamente utilizzato un programma di scanning delle risorse collegate alla rete per verificare che non siano stati connessi apparati e non siano stati installati applicativi non autorizzati.

PC PORTATILI

L'azienda ha dato in dotazione a 40 dipendenti PC portatili. Anche su questi dispositivi è impossibile installare nuovi sw, ed è inibita la possibilità di collegamento a internet da casa.

Tutti i portatili hanno come SO Windows XP che fornisce nativamente funzioni di personal firewalling.

4.3 DB e file system

Le tabelle contenenti dati personali sono separate da quelle che riportano informazioni sensibili. Il collegamento è possibile soltanto tramite un codice applicativo non conosciuto agli utenti.

Nelle tabelle che seguono sono sintetizzati i Data Base gestiti dall'UOSI.

Funzione	Release	Istanza	Livello Availability	Dati Personali	Dati Sensibili	Backup	Applicativo utente
ORACLE							
Anatomia patologica	8.1.7	OLI	Alto	Alto	Alto	Export + fisico	WINSAP
laboratorio Piacenza	8.1.5	DASIT	Alto	Alto	Alto	Export + fisico	HS2000, DASIT
laboratorio Castel S.Giovanni	8.0.5	DASIT	Alto	Alto	Alto	Export + fisico	DASIT
laboratorio Fiorenzuola d'Arda	8.1.5	ORCL	Alto	Alto	Alto	Export + fisico	DASIT
laboratorio Bobbio	9.2.0.3	DASIT	Alto	Alto	Alto	Export + fisico	DASIT
Bilancio/economato/magazzino	8.1.7	ENCO	Medio	Medio	no (?)	Export + fisico	ECP
Bilancio in lire	8.1.7	ENCOPRO	Basso	Medio	no (?)	Export + fisico	BILANCI
Gestione personale: presenze;concorsi;pianta organica;giuridico;assenze;infortuni	9.2.0.3	JOBTIME	Medio	Medio	?	Export + fisico	jobtime
Trattamento economico personale;cococo	8.1.7	paghe	Medio	Medio	si	Export + fisico	master
Veterinari	8.1.7	paghe	Medio	Medio	?	Export + fisico	master
Protocollo delibere con due applicativi	7.3.4	oranad	Medio	Medio	Basso	Export + fisico	nadir
118 emergenza	8.1.7.4.1	J118	Alto	Alto	Alto	export + fisico (?)	ordinari; net118
118 storico emergenze	8.1.7.4.1	W118	Alto	Alto	Alto	export + fisico (?)	STORICO
Pronto soccorso Piacenza	7.3.4	gst	Alto	Alto	Alto	Export + fisico	GST
Pronto soccorso Piacenza	7.3.4	gst	Alto	Alto	Alto	Export + fisico	GST
Pronto soccorso Fiorenzuola d'Arda	7.3.4	gst	Alto	Alto	Alto	Export + fisico	GST
pronto soccorso Bobbio	7.3.4	orcl	Alto	Alto	Alto	Export + fisico	GST
Igiene ambientale(interventi ispettivi presso aziende produttive)	7.3.4						

Funzione	Release	Istanza	Autenticazione	Autorizzazione	Accesso Utenti
MSSQL					
Agenda prenotazione Bobbio	2000 SP	BB_MedsOffice	Applicativo	Applicativo	Applicativo
Screening citologico	2000 SP	Cito	Applicativo	Applicativo	Applicativo
DB anagrafico applicazioni eurosoft	2000 SP	dotSANPiacenza	Applicativo	Applicativo	Applicativo
Cartella Infermieristica	2000 SP	Hs2000	Applicativo	Applicativo	Applicativo
Screening mammografico	2000 SP	Mammo	Applicativo	Applicativo	Applicativo
	2000 SP	MMGConsul	Applicativo	Applicativo	Applicativo
	2000 SP	PazientiHS	Applicativo	Applicativo	Applicativo
assistenza domiciliare	2000 SP	PC_AssDom	Applicativo	Applicativo	Applicativo
registro operatorio	2000 SP	PC_BloccoOperatorio	Applicativo	Applicativo	Applicativo
	2000 SP	PC_cardioAF	Applicativo	Applicativo	Applicativo
Cartella Clinica	2000 SP	PC_Cardiologia	Applicativo	Applicativo	Applicativo
Cartella Clinica	2000 SP	PC_ChirGen	Applicativo	Applicativo	Applicativo
Cartella Clinica	2000 SP	PC_Consultori	Applicativo	Applicativo	Applicativo
Cartella Clinica	2000 SP	PC_Diabetologia	Applicativo	Applicativo	Applicativo
	2000 SP	PC_Elaborazioni			
Cartella Clinica	2000 SP	PC_Endoscopia			
Cartella Clinica	2000 SP	PC_Fisioterapia			
Cartella Clinica	2000 SP	PC_Gastroenterologia			
Agenda prenotazione libera professione	2000 SP	PC_LiberaProfessione			
Cartella Clinica	2000 SP	PC_MalattieInfettive			
Agenda prenotazione Piacenza	2000 SP	PC_MedsOffice			
Cartella Clinica	2000 SP	Pc_OncoEmato			
cartella clinica	2000 SP	Pc_Otorino			
Ticket PS	2000 SP	PC_RecuperoPrestazioni			
	2000 SP	PCP_COMUNE			
DB anagrafico per applicazioni eurosoft	2000 SP	dotSANPiacenza			
Cartella Infermieristica	2000 SP	HS2000			
agenda prenotazione	2000 SP	PC_MedsOffice			
db anagrafico per applicazioni eurosoft	2000 SP	dotSANPiacenza			
gestione laboratori scambio dati	2000 SP	Gelab			
cartella infermieristica	2000 SP	HS2000			
Hospital Web test	2000 SP	HSWebReparto			

Funzione	Release	Istanza	Autenticazione	Autorizzazione	Accesso Utenti
	2000 SP	InsGelabWeb2			
agenda prenotazioni	2000 SP	PC_MedsOffice			
	2000 SP	PCP_COMUNE			
centro trasfusionale	2000 SP	Emodata			
collegamento emodata a strumenti diagnostici	2000 SP	WinStrum			
Fascicolo dipendenti	2000	DossierDipendenti			
intranet aziendale:	2000	LiberaProfessione			
intranet aziendale:	2000	news			
replica news aziendale	2000	NewsDistribution			
accreditamento fornitori	2000	QFornitori			
replica news aziendale	2000	QFornitoriDistribution			
intranet aziendale:	2000	SentPay			
applicativo cup web test	2000	CUP			
db da as 400 test	2000	CUPASPC			
db test	2000	CUPTmp			
db anagrafico per applicazioni eurosoft	2000	dotSANPiacenza			

4.4 Trattamenti automatici

In questo paragrafo vengono descritti i principali applicativi di gestione ospedaliera, istituzionalmente preposti al trattamento della maggior parte dei dati sensibili dell'Azienda. Viene inoltre fornito un elenco completo di tutti gli applicativi censiti e gestiti dall'UOSI.

4.4.1 Applicativi sanitari di gestione ospedaliera

Gli applicativi di tipo sanitario sono prevalentemente installati presso i 4 Ospedali gestiti dall'AUSL non sono collegati in via telematica/informatica e in ogni sede c'è una diversa istanza dell'applicativo e dei DB contenenti i dati personali e quelli sanitari degli assistiti.

I dati, a loro volta, sono trattati dagli applicativi installati presso ciascuna sede.

Ogni ospedale ha il suo laboratorio di analisi "non collegato" a quelli degli altri ospedali.

PRONTO SOCCORSO (PS)

Ognuno dei 4 ospedali ha il proprio Pronto Soccorso, presso il quale è installata un'istanza dell'applicativo, ma solo l'ospedale di Piacenza possiede oltre al Pronto Soccorso Generale, anche quelli Pediatrico, Oculistico ed Ortopedico.

L'applicativo ha 3 macro-funzionalità :

- Inserimento dati di ingresso
- Accettazione ricoveri programmati
- Calcolo scheda dimissione ordinaria (DRG)

All'applicativo si può accedere secondo autorizzazioni differenziate per ruolo professionale e riportate nel sistema di profilazione di Active Directory.

HOSPITAL 2000

È un applicativo presente in tutti gli ospedali, tranne in quello di Bobbio che è molto piccolo. Serve per realizzare la cartella infermieristica che contiene le informazioni necessarie al personale paramedico per controllare giornalmente la somministrazione delle cure e l'effettuazione delle analisi cliniche richieste. Con questo applicativo vengono anche stampate le etichette riportanti in chiaro il nome del paziente ed in codice a barre le analisi richieste con cui vengono identificate le provette da inviare ai laboratori. Se il paziente per il quale vengono effettuate le analisi, è ancora ricoverato, il referto prodotto viene inviato per via informatica al reparto ed aggiunto nella cartella infermieristica. Se la richiesta di analisi è privata, il referto viene stampato e consegnato. Anche in tal caso le tabelle dei dati anagrafici sono separate da quelle dei dati sanitari con identificativo alfanumerico di collegamento tra le due.

ESITO DI ANALISI CLINICHE

I dati relativi all'esito di analisi cliniche vengono prelevati direttamente dagli apparati che effettuano tali analisi e resi disponibili all'applicativo "Hospital2000" che gestisce la cartella infermieristica. Questa soluzione consente di evitare per gran parte il trattamento cartaceo delle informazioni in questione. Il referto è accessibile in sola lettura ed è passato all'applicativo Hospital 2000.

Attualmente questa possibilità è garantita solo all'interno dello stesso ospedale

INFOCLIN

Ogni reparto ha esigenze diverse rispetto alla gestione della cartella clinica. Questo ha comportato che l'applicativo in esame sia distribuito e personalizzato in modo differente a seconda dell'utilizzatore finale. Per questo motivo nel caso in cui un paziente, nell'ambito di uno

stesso ricovero, si trovi a cambiare reparto, la cartella clinica cartacea lo segue mentre quella generata da Infoclin deve essere aperta ex-novo nel nuovo reparto ospitante. È previsto che nel corso del 2005 l'applicativo venga personalizzato e distribuito anche ai reparti di pneumatologia, diabetologia, malattie infettive, otorinolaringoiatria. L'architettura interna dell'applicativo prevede che la tabella dei dati anagrafici sia separata da quella dei dati sanitari ed è previsto un identificativo alfanumerico di collegamento tra le due.

MED'S OFFICE : AGENDA DI REPARTO

Consente la realizzazione di un CUP interno gestito dal reparto per effettuare la prenotazione delle visite mediche. L'output dell'applicativo viene stampato ed ha un formato tale che in un'unica scheda coesistano dati personali e dati sanitari. Le misure di protezione dei dati sensibili e sanitari sono in questo caso realizzate con una opportuna policy di consegna del foglio di prenotazione.

PRENOTAZIONE E ACCETTAZIONE : CUP

Nel Marzo 2005 è stata installata l'applicazione relativa a funzionalità di CUP. Questo sw implementa :

- una modalità di autenticazione basata su tabelle interne che riportano l'elenco delle coppie "ID-Password" cui è autorizzato l'accesso.
- una politica di gestione delle password, che ne forza il cambiamento ogni tre mesi e verifica che la stessa parola d'ordine non venga riutilizzata per almeno cinque cicli.
- Controllo della sessione di lavoro : se il programma non viene utilizzato per più di 20 minuti viene automaticamente attivato uno screen-saver dal quale si può tornare all'applicazione solo tramite reinserimento della password.

MEDICINA DI BASE

Supporta le funzioni scelta e revoca del medico di base. Fa riferimento al DB di "Anagrafe degli assistiti" e gestisce informazioni sulle esenzioni cui hanno diritto i singoli assistiti. Queste ultime non sono riportate in chiaro, ma seguono una precisa codifica.

ANAGRAFICA ASSISTITI

Le funzioni gestite sono :

- inserimento
- cancellazione (logica)
- modifica
- selezione
- stampa liste
- eventuale aggiornamento con anagrafiche comunali

ADI

Gestisce l'agenda degli interventi del personale che si reca a domicilio per prestare assistenza. L'output dell'applicativo viene stampato ed ha un formato tale che in un'unica scheda coesistano dati personali e dati sanitari. Le misure di protezione dei dati sensibili e sanitari sono in questo caso realizzate con una opportuna policy di consegna e gestione del foglio riportante l'agenda.

COMUNICAZIONI CON L'ESTERNO

L'azienda ha un proprio sito internet sul quale sono pubblicati soltanto dati informativi che non hanno nessun riferimento a persone e/o patologie e prestazioni.

Esistono aree riservate accessibili a particolari categorie di collaboratori come :

- Medici di base
- Veterinari
- Comitati consultivi degli utenti

Le comunicazioni **DALL'INTERNO VERSO L'ESTERNO** sono essenzialmente verso la Regione Emilia Romagna; la maggior parte di esse non prevede la trasmissione di dati sanitari personali, ma di informazioni statistiche (screening, dati sull'emofilia,...). I flussi che comportano il trasferimento di dati personali di tipo sanitario seguono i criteri di sicurezza e protezione delle informazioni esplicitamente indicati dalla Regione, che, in linea generale prevedono invii separati dei file contenenti le informazioni anagrafiche rispetto a quelli che contengono informazioni sanitarie. La ricostruzione della coppia "assistito-patologia" è possibile solo tramite dei codici di correlazione.

Le comunicazioni alla Regione riguardanti prestazioni di trapianto di midollo, che rientrano nella categoria dei dati di tipo genetico, sono effettuate tramite VPN (quindi crittografate), secondo le indicazioni tecniche della Regione stessa.

Nel corso del 2005 è prevista la partenza di due progetti che comportano la trasmissione di dati sanitari personali : tele-elettrocardiogramma e telecontrollo dei coagulometri. In entrambi i casi le informazioni sono inviate senza il nome del paziente, ma accoppiate a un codice che lo identifica.

Tra i soggetti che instaurano un flusso di comunicazione **DALL'ESTERNO VERSO L'AUSL** ci sono i farmacisti, gli sportelli comunali e particolari studi medici di Medicina Generale che effettuano prenotazioni di analisi cliniche e scelta e revoca dei Medici di Base.

Attualmente il flusso delle richieste di prenotazione (veicolato mediante programmi che sfruttano la tecnologia Internet), viene ricevuto dai server in DMZ e, solo dopo il passaggio attraverso un firewall opportunamente configurato, passa al server di produzione. In ogni caso il sistema non permette di rivedere le prenotazioni effettuate ed una eventuale disdetta può essere comunicata solo telefonicamente.

Dal mese di maggio di quest'anno l'accesso da remoto viene reso ancor più sicuro con l'adozione di tecniche di autenticazione forte tramite l'utilizzo di smart-card che saranno distribuite ai farmacisti. Per preparare opportunamente lo startup del progetto dal 16 Marzo inizieranno le attività di formazione degli utenti finali.

Ai fornitori non sono mai stati affidati dati reali per eseguire prove sulle loro piattaforme. Nel caso se ne dovesse ravvisare la necessità è prevista una procedura di richiesta scritta che verrà soddisfatta soltanto dopo aver reso anonimi i dati stessi.

Nelle tabelle che seguono sono indicate le istanze di tutti gli applicativi utilizzati.

	Funzionalità	Descrizione	Istanza
Screening2000	Screening citologico	Invito ad effettuare il paptest per le donne che hanno superato i 40 anni di età	Cito
	Screening mammografico	Invito ad effettuare la mammografia per le donne che hanno superato i 45 anni di età	Mammo
Hospital 2000	Cartella Infermieristica	Permette di redigere la cartella infermieristica	Hs2000
ADI	Assistenza Domiciliare Infermieristica	Assistenza Domiciliare Infermieristica	PC_AssDom
Esalab	Statistiche	Attinge al DB per effettuare le statistiche relative ai dati trattati da tutti gli applicativi	PC_Elaborazioni
Infoclin	Cartella Clinica Consultorio	Informazioni sanitarie complete sulle persone che accedono al consultorio	MMGConsul
	Registro Operatorio	Registro presente nella sala operatoria e contenente tutte le informazioni sul paziente operato, i medicinali somministrati e tutto ciò che è stato utilizzato per l'intervento.	PC_BloccoOperatorio
	Cartella Clinica	Cartella clinica con i dati specifici del reparto	PC_Cardiologia
			PC_ChirGen
			PC_Consultori
			PC_Diabetologia
			PC_Endoscopia
			PC_Fisioterapia
			PC_Gastroenterologia
			PC_MalattieInfettive
			Pc_OncoEmato
			Pc_Otorino
Med's Office	Agenda prenotazione	Agenda prenotazioni per l'ospedale di Piacenza	PC_MedsOffice
		Agenda prenotazioni per l'ospedale di Bobbio	BB_MedsOffice
		Agenda prenotazioni per la libera professione	PC_LiberaProfessione
Recupero-prestazioni	Pagamento ticket per chi viene dimesso dal PS con codice bianco o giallo.	E' utilizzato negli uffici preposti al recupero dell'importo relativo alle prestazioni erogate sui pazienti che non avrebbero avuto necessità di transitare per il PS.	PC_RecuperoPrestazioni

	Funzionalità	Descrizione	Istanza
Hospital Web	Scambio dati con laboratori	Interfacciata tra Hospital Web e i laboratori DASIT	Gelab
	Inserimento delle richieste per i laboratori	Interfaccia tra Hospital Web e Dasilab (applicazione di laboratorio)	InsGelabWeb2
Hospital Web test	Hospital Web test	Versione di test della nuova release di Hospital2000	HSWebReparto
Emodata	Centro Trasfusionale	Gestione dei pazienti del centro trasfusionale	Emodata
WinLab	Centro Trasfusionale	Gestione dei referti emessi dal laboratorio di analisi cliniche interno al centro trasfusionale	WinLab
WinStrum	Collegamento di Emodata agli strumenti diagnostici	Collega il referto diagnostico degli apparati che effettuano le analisi con l'anagrafica pazienti del cenì del centro trasfusionale	WinStrum
Fascicolo del personale	Fascicolo dipendenti	Applicativo web con cui si raccolgono informazioni sui dipendenti	DossierDipendenti
	Fascicolo liberi professionisti	Applicativo web per registrare i dati che servono per autorizzare i dipendenti all'esercizio della libera professione	LiberaProfessione
NEWS	Inserimento delle news sulla intranet	Aplicativo web necessario per inserire le news on line (intranet)	news
	Inserimento della replica delle news sul sito aziendale (internet)	Aplicativo web necessario per inserire le news on line (internet)	NEWSReplica
Qualifica fornitori	Inserimento informazioni sui fornitori	Accreditamento dei fornitori	QFornitori
SentPay	Richiesta di mandati plurimi	Permette la richiesta di mandati plurimi al tesoriere	SentPay
Sipra	Gestione delle squadre antiincendio	Permette di gestire l'antincendio	Sipra
Valutazione del personale	Gestione dei percorsi formativi dei dipendenti	Gestisce le informazioni relative al livello di formazione scolastica, accademica e a quella acquisita durante corsi di aggiornamento professionale. Facilita il disegno del percorso formativo futuro.	Valutazione del personale
CUP	Centro Unico di Prenotazione	Applicativo che realizza funzionalità CUP via web.	CUP
ADS	Gestione medici di base	Assegnazione e revoca del medico di base all'assistito.	
Anagrafica Assistiti	Gestione dell'anagrafica assistiti	Inserimento, variazione e cancellazione delle informazioni anagrafiche relative agli assistiti.	
Gepadial	Gestione Nefrologia	Gestione pazienti del reparto di Nefrologia	
3Pstudio	Gestione Servizio Salute Mentale	Gestione SI del servizio di salute mentale	
Gias	Gestione SERT	Gestione assistiti tossicodipendenti	N.A. (file a indici)

	Funzionalità	Descrizione	Istanza
WINSAP	Anatomia patologica (esami eseguiti presso Anatomia Patologica richiesti dagli ospedali della AUSL o da soggetti esterni)		OLI
HOSPITAL2000, DASIT	lab pc		DASIT
DASIT	lab csg		DASIT
DASIT	lab fda		ORCL
DASIT	lab bob		DASIT
ECP	bilancio/economato/magazzino		ENCO
BILANCI	bilancio in lire		ENCOPRO
jobtime	gestione personale: presenze;concorsi;pianta organica;giuridico;assenze;infortuni		JOBTIME
master	trattamento economico personale;cococo		paghe
master	veterinari		paghe
nadir	protocollo delibere con due applicativi		oranad
ordinari; net118	118 emergenza		J118
STORICO	118 storico emergenze		W118
gst	Pronto soccorso PC		gst
gst	Pronto soccorso PC		gst
gst	Pronto soccorso fda		gst
gst	pronto soccorso bobbio		orcl

4.5 Trattamenti non automatici

Le varie unità organizzative dell'azienda trattano le informazioni personali e sensibili secondo innumerevoli modalità non automatizzate, di seguito vengono descritte le principali, con particolare attenzione a quelle che sono state in qualche misura proceduralizzate.

4.5.1 Trattamenti cartacei

Le attività dell'Azienda USL di Piacenza prevedono un gran numero di trattamenti che si avvalgono di supporti cartacei.

Tutte le UOA gestiscono i propri archivi cartacei, che vengono trattati secondo le indicazioni generali fornite dall'Amministrazione in merito alla sicurezza fisica e alle autorizzazioni per l'accessibilità dei documenti.

- Scheda ambulanza : viene redatta dal personale d'ambulanza e riporta i segni vitali del paziente. Una copia è consegnata al personale di triage del pronto Soccorso.
- Scheda triage : viene stampata una scheda riportante l'anagrafica, la sintomatologia e l'urgenza valutata, con l'indicazione dello specialista cui sottoporre il paziente. La scheda viene consegnata a mano al medico di pronto soccorso, che inserisce i dati sanitari nell'applicativo PS
- Scheda dell'ufficio accettazione del Pronto Soccorso : viene stampata dal relativo programma per essere consegnata "brevi manu" al reparto cui viene indirizzato il paziente. Una volta terminata l'ospedalizzazione la stessa scheda, compilata con le cure e le prestazioni somministrate, viene passata all'ufficio DRG che inserisce nel suo applicativo i dati relativi alle prestazioni per richiedere il rimborso alla Regione. Il DRG non ha dati direttamente riconducibili alla malattia del singolo paziente (a meno dell'indicazione del reparto di ricovero)
- Scheda infermieristica : viene stampata giornalmente e utilizzata dal personale paramedico per effettuare una operazione di "lista e spunta" delle cure e delle analisi cui debbono essere sottoposti i pazienti di reparto.
- Etichettatura delle provette per analisi del sangue : vengono stampate giornalmente le etichette che il personale del reparto richiedente applica sui contenitori che vengono inviati ai laboratori di analisi. Le etichette riportano in chiaro il nome e cognome del paziente, mentre la tipologia di analisi richiesta è riportata in codice a barre interpretabile direttamente solo dalla macchine che eseguono le analisi. Attualmente questa procedura viene seguita
- Refertazione di analisi e prestazioni Attualmente l'esito di una analisi clinica o di una prestazione medica (visita presso altro reparto, consulenza, ecc,) anche se disponibili sul SI vengono comunque consegnate su supporto cartaceo. Questo perché, per motivi legali, è necessaria la firma di chi ha stilato il referto.
- Archiviazione cartelle cliniche
Dopo la dimissione del paziente le cartelle cliniche rimangono in reparto per un tempo che varia, a seconda della patologia, dai tre ai dodici mesi. Al termine di questo periodo vengono raccolte in apposite scatole di cartone, chiuse in modo da non essere accessibili a non autorizzati e poi ritirate dal personale dell'azienda appaltante. I plichi non sono immediatamente consultabili dal vettore o da chiunque altro durante il trasferimento e vengono trasportati dal corriere su veicoli controllati e chiusi a chiave.
Le cartelle cliniche sono conservate presso l'archivio della SEAC sito in Cremona.
Una volta giunte a destinazione le scatole sono archiviate per data di dimissione, criterio con il quale se ne richiede l'identificazione a fronte di richieste da parte dell'AUSL.
Le cartelle sono conservate per un periodo indefinito.
- Richiesta copia cartacea della cartella clinica
Copia della cartella clinica può essere richiesta :
 - Allo sportello
 - Per fax
 - Per telefono

A fronte di una richiesta viene inviata una segnalazione alla SEAT che si occupa di fornire una copia fotostatica, che viene poi trasportata secondo le modalità di legge in contenitori dotati di serratura o equipollenti.

Una volta giunta presso l'ufficio competente, la copia della cartella viene consegnata, chiusa in una busta, ai soli interessati o a chi presenti opportuna delega. Può anche essere spedita in busta chiusa all'indirizzo dell'interessato, di chi ha delega o degli eredi.

- Schede di prenotazione
Sono consegnate ai soli interessati
- Schede di pianificazione degli interventi domiciliari
Sono consegnate ai soli incaricati che le utilizzano per le loro attività. Non esiste alcuna forma di archiviazione perché, terminata la prestazione, le schede vengono distrutte.
- Ricettario

4.5.2 *Trattamenti tramite telefono o radio*

L'Azienda USL di Piacenza gestisce direttamente il 118, che riceve segnalazioni **PER VIA TELEFONICA** di situazioni e persone presso le quali intervenire con mezzi sanitari in grado di portare un primo soccorso e/o trasportare eventuali feriti o ammalati.

Per motivi di sicurezza tutte le chiamate telefoniche sono registrate e conservate su DAT presso i locali del centro operativo. Per poter intervenire anche in situazioni d'estrema urgenza esiste inoltre un sistema in grado di identificare qualsiasi numero chiamante (anche se volutamente mascherato). Non esiste invece alcun sistema d'identificazione della cella del chiamante che dia indicazioni sul suo posizionamento fisico. In ogni caso, una volta verificato che non esista la condizione di utilizzo del numero chiamante (es. un paziente che, a causa della gravità del suo stato, non sia riuscito a terminare la propria segnalazione) questo ultimo viene immediatamente cancellato.

Una volta ricevuta la segnalazione gli operatori del 118 raggiungono **VIA RADIO** il mezzo di zona (esiste un'associazione statica tra ambulanza e territorio di competenza) e, se necessario, l'elicottero destinato al trasporto di personale specializzato.

La comunicazione radio non è crittata, ma esiste una formale procedura per cui al personale di ambulanza viene comunicato, quando possibile, soltanto l'indirizzo con un numero di citofono, in modo da non poter fare una diretta associazione tra la l'evento per cui vengono mobilitati e la persona coinvolta.

Comunicazioni telefoniche dalla AUSL. Esiste una specifica procedura che regola le comunicazioni telefoniche riguardanti cure e prestazioni (es. annullamenti o rinvii), presso il numero fisso dell'assistito. L'utilizzo del numero cellulare avviene solo dietro esplicito dell'interessato.

4.5.3 *Comunicazioni verbali*

Per sua missione l'Azienda si trova in molte occasioni a trattare dati sensibili sotto forma di comunicazioni verbali. I possibili soggetti che, oltre all'interessato, cui possono essere comunicate informazioni riservate in questa modalità sono tutti quelli indicati nel paragrafo "Soggetti cui si riferiscono i dati".

5. **GESTIONE COLLABORATORI ESTERNI**

L'Azienda si avvale di collaboratori a vario titolo che frequentano i propri siti e gli assistiti. Tra questi possiamo citare :

- fornitori di beni e servizi
- volontari
- studenti delle scuole interne
- tirocinanti
- associazioni senza scopo di lucro

- badanti
- cappellani

Considerando che tutte queste figure, in diverse modalità, possono venire a conoscenza di informazioni sensibili, l'AUSL di Piacenza ha provveduto a emettere comunicazioni che informano e regolarizzano le loro attività nel rispetto della 196.

5.1 Lettera ai fornitori

E' stata redatta una lettera tipo da inviare ai fornitori di hardware e software, per richiedere l'adeguamento ai requisiti minimi di sicurezza richiesti dalla 196. Come da allegato 5 la lettera prevede una risposta formale da parte dei fornitori, nella quale venga dichiarata la data entro la quale viene garantita la conformità.

6. ANALISI DEI RISCHI

È stata effettuata un'analisi dei rischi, focalizzata sulle circostanze possibili o probabili che possono verificarsi e che possono comportare la diffusione non autorizzata, la distruzione o perdita, anche accidentale delle informazioni, l'accesso non autorizzato od il trattamento non consentito o non conforme alle finalità della raccolta (art. 15 della legge 675/96 ed art. 31 del D. Lgs. 196/2003).

Scopo dell'analisi del rischio è identificare le cause più probabili di rischio per l'Azienda, valutare il grado d'esposizione e determinare quali misure di sicurezza, quante e in che modo debbano essere realizzate.

Il numero di elementi di rischio, per il quale si rende necessaria l'attuazione di adeguate misure di sicurezza, dipende dal grado di esposizione al rischio che si è disposti a tollerare.

Si può identificare, così, una soglia che suddivida i rischi in accettabili, per i quali non è conveniente realizzare alcuna misura di sicurezza, e non tollerabili, per i quali invece è necessario determinare un certo numero di misure di sicurezza, che dovranno essere implementate secondo un piano ben definito.

Di seguito vengono riportati in sintesi i risultati dell'analisi effettuata nel corso del 2004.

I rischi analizzati sono stati individuati, classificati e descritti raggruppandoli secondo i seguenti principali criteri

- **AMBIENTALI**
- **INTEGRITÀ** : intesa come la gestione dell'accuratezza e completezza delle informazioni e delle relative applicazioni, la salvaguardia della esattezza dei dati, la difesa da manomissioni o modifiche non autorizzate, ecc.;
- **RISERVATEZZA** : intesa come la garanzia che le informazioni siano accessibili solo alle persone autorizzate, la protezione delle trasmissioni, il controllo degli accessi, ecc.;
- **DISPONIBILITÀ** : intesa come garanzia che l'informazione sia disponibile, quando necessario, alle persone autorizzate, evitando la perdita o il degrado dei dati e dei servizi
- **SPECIFICI** sono stati prudentemente aggiunte valutazioni circa ulteriori possibili rischiosità in relazione a trattamenti riferiti a dati diversi da quelli sensibili e giudiziari, che possono presentare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

L'esame dei rischi è stato fatto anche in relazione alla natura dei dati, distinguendo tra i dati personali comuni e particolari (sensibili, giudiziari), ed in relazione alle caratteristiche del trattamento.

I rischi esaminati sono stati individuati, classificati e descritti nei seguenti principali raggruppamenti:

6.1 Rischi che incombono sui dati

6.1.2 Rischi ambientali

Sono considerati come rischi ambientali quelli derivanti dalla collocazione territoriale dei diversi siti dell'Azienda, e quindi l'ubicazione dei luoghi in cui vengono custodite e trattate le diverse informazioni.

In dettaglio sussistono le condizioni per confermare che :

- La zona di operatività è ubicata in fascia territoriale geografica che, nelle carte di pericolosità sismica (anche quelle di più recente divulgazione) non risulta classificata tra le zone a grado di pericolosità elevato o medio. In ogni caso occorre segnalare nella Provincia di Piacenza si segnalano deboli scosse sismiche, l'ultima delle quali il 21 Settembre 2004 (Volpara e Golferenzo del 3°-4° grado Mercalli, equivalente a 3,1 Richter).
- Entro il 2005 è previsto il trasferimento del CED UOSI presso il primo piano di una sede collocata in zona più vicina al Po di quanto non sia l'attuale. Il fiume in occasione di eccezionali eventi atmosferici potrebbe esondare. L'esperienza degli ultimi decenni, e segnatamente quella verificata nell'Ottobre e Novembre 2000, quando nelle province di Piacenza, Parma, Reggio Emilia, Modena e Bologna si sono verificati alluvioni e dissesti idrogeologici, ha dimostrato che le strutture sono risultate sufficientemente robuste rispetto a questo rischio. L'unico sito interessato è stato il polo chirurgico, in cui si è verificato un allagamento del piano -1.
- A Caorso, dove è situato anche un ufficio CUP dell'AUSL, è presente un impianto nucleare, attualmente disattivato e per cui è previsto lo smantellamento e la sanificazione entro il 2016. Al momento non è prevedibile se e quanto queste operazioni potranno influenzare il rischio di emissioni radioattive.

In generale, non risultano rischi specifici prevedibili e probabili, correlati alla ubicazione geografica del centro di elaborazione dei dati e dei diversi siti della AUSL.

6.1.3 Integrità dei dati

Il concetto di "integrità" è stato riferito, sulla base delle definizioni convenzionali, alla correttezza ed alla consistenza dei dati. Pertanto, l'accertamento dell'integrità dei dati ha riguardato la protezione da rischi di possibili modifiche o distruzione accidentali o deliberate.

L'esame dei rischi possibili circa le minacce all'integrità dei dati sono stati classificati in:

- rischi di natura accidentale;
- rischi da programmi di cui all'art.615 quinquies del codice penale;
- rischi di carattere volontario.

La ricognizione ha riguardato attualmente le strutture informatiche dello UOSI, che opera in modalità centralizzata e interviene sui dati residenti presso gli altri siti.

RISCHI DI NATURA ACCIDENTALE

Per i dati trattati elettronicamente

Riguardano l'involontaria sovrascrittura o distruzione dei dati, imputabili ad azioni umane errate oppure a guasti, malfunzionamenti o interruzioni nel funzionamento delle apparecchiature dedicate alla memorizzazione.

- comandi applicativi errati (a causa di applicazioni non testate in maniera sufficiente);

- comandi operativi errati (per sequenze non documentate o eseguite da personale non sufficientemente addestrato);
- malfunzionamenti hardware (es: guasto delle testine di un pacco di dischi);
- deterioramento nel tempo dei supporti di memorizzazione e del mezzo fisico che li ospita;
- software pericoloso, in particolare virus dei computer o utilizzo di routine tipo "superzap";
- mancanza o interruzione di alimentazione elettrica, dovuta a black-out del fornitore del servizio;
- eventi disastrosi che superino i livelli ipotizzati all'atto della stesura delle contromisure.

Per i dati trattati su supporto cartaceo

Rientrano in questa categoria i rischi dovuti a :

- distruzione di documentazione per : incendio, allagamento, umidità,
- errori umani nell'archiviazione cartacea dei documenti (scambio di referti, cartelle cliniche,etc.)
- modifica non volontaria di documenti non pertinenti (scambio di documenti)

Per i dati trattati verbalmente

Rientrano in questa categoria i rischi dovuti a :

- comunicazioni non supportate da documentazione oggettiva (scambio di paziente)

RISCHI DA PROGRAMMI DI CUI ALL'ART. 615 QUINQUIES DEL C.P.

I rischi connessi alla diffusione dei virus e dei programmi pericolosi sono stati così individuati :

- corruzione dei file eseguibili e, a volte, dei dati;
- corruzione di documenti;
- perdita di file;
- perdita di spazio utilizzabile nelle memorie;
- cattivi funzionamenti del sistema;
- degrado delle prestazioni del sistema;
- impossibilità di utilizzo del sistema;
- responsabilità legali in violazione all'art.615 quinquies del codice penale;
- perdita di reputazione verso i soggetti esterni.

Tra i più recenti pericoli, si è inoltre aggiunta la creazione di nuovi virus che colpiscono i programmi eseguibili di Windows (es: suite Office di Microsoft), e di programmi (chiamati "backdoor" o "hacktools") che consentono l'amministrazione remota della rete potendo essere installati sui PC senza che l'operatore se ne accorga (come i virus) e che, una volta attivati, consentono collegamenti via TCP/IP permettendo ad intrusi di manipolare e controllare varie funzioni del PC. Questi programmi pericolosi non sono propriamente definibili virus o cavalli di Troia, ma, ai fini della prevenzione dai rischi, devono essere considerati con molta attenzione in considerazione della loro capacità di diffondersi in rete e di consentire azioni illegali.

Si è considerato che i virus ed i programmi pericolosi potrebbero penetrare nei computer aziendali tramite:

- supporti infettati provenienti da terzi;
- supporti infettati importati dai dipendenti senza l'autorizzazione dell'azienda;
- file scambiati in rete.

RISCHI DI CARATTERE VOLONTARIO

Per i dati trattati elettronicamente

Ci si è riferiti alle alterazioni dell'integrità conseguenti ad un'eventuale azione deliberatamente perpetrata allo scopo di :

- leggere indebitamente dati riservati,
- modificare volontariamente i dati,

- inserire nuovi dati,
- distruggere i dati.

Riguardano la sovrascrittura o distruzione dei dati, imputabili ad azioni umane

- comandi operativi pericolosi (es. cancellazioni, copie, installazioni di sw pericolosi)
- interventi sull' hardware (es: spegnimenti volontari delle unità di elaborazione, furti di supporti di memorizzazione);
- installazione di software pericoloso (sniffer, etc.)
- "furto di identità elettronica"
- modifica non autorizzata di dati e documenti

Per i dati trattati su supporto cartaceo

Rientrano in questa categoria i rischi dovuti a :

- distruzione o furto di documentazione,
- modifica volontaria di documentazione da parte di personale non autorizzato o per scopi non leciti

Per i dati trattati verbalmente

Rientrano in questa categoria i rischi dovuti a :

- comunicazioni carenti o erronee agli interessati e a terzi per cui esista chiaro consenso

6.1.4 Riservatezza dei dati

Per quanto attiene la "riservatezza" si è fatto riferimento alla natura ed al grado di confidenzialità, riservatezza e particolarità dei dati, al fine di garantire il dovuto e necessario riserbo sulle informazioni proteggendole da eventuali accessi e/o divulgazioni non autorizzate, consentendone l'utilizzo ed il trattamento solamente ai soggetti incaricati.

Nel corso del 2005 è prevista l'adozione di apparati **biometrici** per il controllo accessi fisici alle sale CED. Una volta espletate le opportune procedure d'acquisto, verrà effettuata dettagliata notifica al Garante e saranno messe a punto le relative misure di protezione sui dati biometrici degli interessati.

Il rischio sulla riservatezza delle informazioni è stato esaminato in relazione alla possibilità che si realizzino, in qualunque forma, rilasci di informazioni a non autorizzati e/o accessi non autorizzati ai dati.

Gli eventi controllati posti in relazione al rischio di accessi non autorizzati sono stati determinati sulla base delle seguenti fattispecie :

- rischi di accessi fraudolenti dall'interno;
- rischi di accessi fraudolenti dall'esterno;
- rischi derivanti da trattamenti non consentiti o non conformi alle finalità della raccolta.

RISCHI DI ACCESSI FRAUDOLENTI DALL'INTERNO

Per i dati trattati elettronicamente

Rientrano in questa categoria i rischi dovuti a :

- "profilo" di autorizzazione all'accesso non aderente al ruolo assegnato o conseguente all'attribuzione di "privilegi" di accesso eccessivi;
- "inferenza", ossia alla cattura di un campione di informazioni che, correlate tra loro, consentano di giungere alla conoscenza indiretta di dati;
- utilizzo dei privilegi di "Amministratori di Sistema" per l'accesso ad archivi (su HOST auditabile);
- "furto di identità elettronica" di un dipendente autorizzato all'accesso ai sistemi;
- "manomissione" delle autorizzazioni da parte del personale addetto al controllo ed all'amministrazione dei profili di accesso.

Per i dati trattati su supporto cartaceo

Rientrano in questa categoria i rischi dovuti a :

- mancata tutela, furto, smarrimento della documentazione “in uso”; (es documentazione contenente dati sensibili, lasciata in vista di eventuali terzi non autorizzati)
- mancata tutela, furto, smarrimento della documentazione archiviata.

Per i dati trattati verbalmente

Rientrano in questa categoria i rischi dovuti a :

- colloqui tenuti con o in presenza di terzi non autorizzati
- Tecniche di social engineering per ottenere autorizzazioni non previste (es. richiesta della password di colleghi o di informazioni per ricostruirla facilmente)

RISCHI DI ACCESSI FRAUDOLENTI DALL'ESTERNO

Per i dati trattati elettronicamente

Rientrano in questa categoria i rischi dovuti :

- accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software;
- “furto di identità elettronica” di un dipendente autorizzato all’accesso remoto ai sistemi;
- intercettazione di comunicazioni telematiche,
- accessi tramite collegamenti alle reti (Internet ed Intranet) da parte di operatori esterni (Hackers) con intenzioni amichevoli od ostili.

Per i dati trattati su supporto cartaceo

Rientrano in questa categoria i rischi dovuti a :

- mancata tutela, furto, smarrimento della documentazione “in uso”;
- mancata tutela, furto, smarrimento della documentazione archiviata.

Per i dati trattati verbalmente

Rientrano in questa categoria i rischi dovuti a :

- intromissione di soggetti non autorizzati in zone o locali in cui si svolgono conversazioni su informazioni riservate

RISCHI DERIVANTI DA TRATTAMENTI NON CONSENTITI O NON CONFORMI ALLE FINALITÀ DELLA RACCOLTA

Sono state ricercate le circostanze che richiedono trattamenti di dati personali per i quali è necessario ottenere un preventivo consenso al fine di escludere che in Azienda possano essere effettuati, anche involontariamente, trattamenti di tali dati senza averne il consenso.

Pertanto, l’attenzione è stata rivolta in particolare alle circostanze organizzative nelle quali, a causa di una possibile, pur se improbabile, gestione non corretta dei “consensi frazionati” e dei “non consensi” avvengano trattamenti non conformi alle finalità

6.1.5 Disponibilità dei dati

Il concetto di “disponibilità” si riferisce alla necessità ed al conseguente diritto dei soggetti interessati, che i dati personali e sanitari possano essere trattati, nei limiti di tempo legati al raggiungimento dello scopo per cui sono stati raccolti, in tutte le forme e le circostanze lecite e previste.

L’obiettivo di questo criterio è fare in modo che i dati e le informazioni siano disponibili al momento di una richiesta effettuata da coloro che sono in possesso delle autorizzazioni necessarie. La disponibilità è stata valutata sia per gli utenti esterni (prevalentemente gli assistiti) che per quelli interni incaricati del trattamento.

I rischi di non disponibilità sono stati esaminati in relazione ad eventi di natura accidentale o intenzionale.

RISCHI DI CARATTERE ACCIDENTALE

In questa famiglia di rischi è stata compresa l'eventualità che le informazioni non siano disponibili a causa di eventi non volontari e/o non previsti, dovuti a:

Per i dati trattati elettronicamente

- mancanza di alimentazione elettrica, dovuta a black-out del fornitore del servizio;
- problemi relativi all'hw (p.e. guasti alle unità di elaborazione, di memorizzazione o di trasmissione);
- anomalie in programmi che avrebbero dovuto elaborare i dati e che non hanno potuto completare la loro esecuzione (p.e. a causa di errori di procedure per input errati, o errori di implementazione);
- errate azioni del personale incaricato che impediscono l'accesso alle informazioni (p.e. mancata copia di un archivio o mancato montaggio di un supporto);
- dimensionamento non sufficiente delle risorse tecnologiche deputate alla trasmissione ed alla memorizzazione.

Per i dati trattati su supporto cartaceo

- irreperibilità della documentazione cartacea per perdita, furto a opera di terzi, distruzione, smarrimento
- tempi di reperimento della documentazione cartacea non congruenti con le effettive necessità di trattamento

Per i dati trattati verbalmente

- indisponibilità del personale che possiede l'informazione
- carenza dei flussi informativi autorizzati (l'informazione non perviene nei tempi e nei modi congruenti al trattamento per cui è stata rilevata)

RISCHI DI CARATTERE INTENZIONALE

In questa tipologia di rischi rientrano le fattispecie in cui le informazioni non sono disponibili a causa di azioni umane volontarie, poste in essere con lo scopo preciso e determinato di impedire l'accesso alle informazioni da parte dei soggetti che detengono il pieno diritto di farlo.

Per i dati trattati elettronicamente

- danneggiamento o manomissione delle attrezzature sia hw che sw
- danneggiamento o manomissione delle connessioni.

Per i dati trattati su supporto cartaceo

- furto da parte di personale interno della documentazione cartacea
- volontario danneggiamento e/o distruzione della documentazione cartacea
- volontario occultamento della documentazione cartacea

Per i dati trattati verbalmente

- rifiuto o reticenza nel comunicare l'informazione all'interessato a ad aventi diritto
- generica infedeltà o comunque, negligenza e/o disobbedienza del personale addetto al controllo ed alla amministrazione delle informazioni;

6.1.6 Ulteriori rischi di cui all'art.615 ter del codice penale

Oltre ai precedenti rischi che gravano sulla integrità, disponibilità e riservatezza dei dati trattati, sono stati considerati ulteriori elementi quali:

- **L'ACCESSO ABUSIVO**, ovvero che un eventuale intruso si insinui all'interno dei siti controllati (CED, Laboratori, etc) o comunque si trattenga in una qualsiasi area oltre l'orario consentito e contro volontà di chi ha il diritto di escluderlo.

Gli accessi abusivi riguardano sia chi potrebbe penetrare illecitamente nel sistema AUSL, o in parte di esso, dall'interno dell'azienda (insider), sia chi si introduce dall'esterno dell'organizzazione aziendale.

Gli accessi abusivi comportano sia rischi connessi alle violazioni di legge, sia altri rischi diretti e indiretti di tipo tecnico, operativo, legale e di reputazione dell'azienda colpita.

Più analiticamente i rischi riguardano :

- Conoscenza dei dati a persone non autorizzate.
- Distruzione e perdita totale o parziale dei dati.
- Danneggiamento dei dati.
- Diffusione di documenti, comuni e riservati.
- Negazione o degrado del servizio agli utenti
- Impossibilità di svolgere correttamente i trattamenti (es. la presenza illecita di terzi può impedire la diretta comunicazione all'interessato)
- Diffusione di programmi informatici infetti.
- Mal funzionamento di programmi.
- Rallentamento delle capacità del sistema.
- Perdita di tempo.
- Pubblicazione di notizie nocive all'immagine e reputazione dell'azienda.
- Sequestro di mezzi informatici.
- Violazioni di leggi, regolamenti (e per alcuni settori le istruzioni di vigilanza).

Per i dati trattati elettronicamente

Si è considerata la circostanza che il sistema sia configurato in maniera da consentire l'accesso solo tramite parole chiave eventuale associate a codici identificativi (user ID), ed al fatto che alla robustezza delle chiavi e ai codici di ingresso non viene riservata la dovuta attenzione, così i codici sono facilmente ricavabili e le parole chiave calcolabili in breve tempo. Tutti i sistemi protetti da parole chiave deboli o addirittura predefinite sono facilmente attaccabili.

I sistemi telematici funzionano e comunicano tra loro attraverso canali di comunicazione che, all'ingresso nel domicilio informatico del proprio sistema assumono il nome di porta. Le porte sono molte ed hanno precise funzioni. Molti utenti ne ignorano l'esistenza e le lasciano attive, cioè aperte, anche quando non sono necessarie per i propri motivi di lavoro. Queste porte, involontariamente lasciate aperte costituiscono una delle maggiori criticità, quindi rappresentano potenziali vulnerabilità del sistema da correggere.

Gli accessi abusivi a un sistema protetto sono facilitati dalle debolezze del sistema, dalle cosiddette vulnerabilità. Le vulnerabilità possono riguardare i sistemi operativi, i protocolli, le applicazioni, qualunque software in genere, il sistema fisico, il sistema delle trasmissioni.

Le vulnerabilità, se sfruttate, danno origine a diverse tipologie d'attacco, le più comuni individuate nell'analisi dei rischi riguardano :

- **RICERCA DELLE PASSWORD** Sono metodi con i quali è possibile trovare i codici d'accesso o loro parti, mediante l'utilizzo di dizionari o programmi automatizzati detti "brute force tools". Questi programmi si basano sul tentativo di entrare nei sistemi provando in sequenza milioni di combinazioni diverse. Le parole chiave possono del resto più semplicemente essere individuate con sistemi che nulla hanno a che fare con la tecnologia, detti di "social engineering" (es. leggendo sui supporti cartacei dove gli incaricati le hanno trascritte per non dimenticarle, domandando informazioni personali sull'incaricato al trattamento che interessa da cui ricostruirle facilmente, telefonando a un call center fingendosi un personaggio importante che ha scordato la sua parola segreta, etc)
- **INTERCETTAZIONI DI DATI** Il metodo consiste nel tentativo di intercettare i dati, o meglio i cosiddetti pacchetti scambiati nella rete. Se un pacchetto è intercettato e copiato sarà possibile ricavarne molte informazioni, tra esse
 - l'identificativo del server di trasmissione,
 - il nome dell'utente
 - la password ad esso associata.

- **RICERCA DI FILE CON ACCESSO PRIVILEGIATO** Si tratta di un tipologia di attacco indirizza a reti con sistemi operativi che nell'ambito delle possibilità gestionali prevedono meccanismi di accesso privilegiato al sistema.
- **AZIONI VERSO IL PROTOCOLLO IP** Si tratta di metodi finalizzati ad ottenere il dirottamento dei dati in transito sulla rete sotto forma di pacchetti IP verso false destinazioni simulando (impersonificando) un host di destinazione.
- **DIROTTAMENTO DI SESSIONI** Sono una variante degli attacchi al protocollo IP finalizzata all'esportazione di dati dal flusso di pacchetti.
- **PREVISIONE DI SEQUENZE DI NUMERI** La connessione tra host via TCP-IP avviene mediante scambio di un pacchetto di connessione che include una sequenza di numeri; in certi sistemi tali numeri sono riproducibili mediante algoritmi noti.
- **SOSTITUZIONE DELLE LIBRERIE CONDIVISE** Una libreria condivisa è costituita da un gruppo di funzioni che il sistema operativo assume su richiesta di un programma informatico. L'attacco consiste nel sostituire le librerie ufficiali con nuove funzioni modificate di proposito che permettono l'intrusione nel sistema.

Per i dati trattati su supporto cartaceo

La presenza di estranei nei locali in cui vengono trattati documenti riservati (come referti clinici di qualsiasi natura, fax, documentazione in uso e consultazione, documentazione archiviata in contenitori locali) può essere estremamente pericolosa per la salvaguardia dei criteri di integrità, riservatezza e disponibilità.

Per i dati trattati verbalmente

La presenza non desiderata o non avvertita di estranei nei locali in cui vengono scambiate informazioni riservate può essere estremamente pericolosa per la salvaguardia dei criteri di integrità, riservatezza e disponibilità.

6.2 Riepilogo dell'analisi dei rischi

La tabella seguente riepiloga gli eventi considerati nell'analisi dei rischi esposta nei paragrafi precedenti, la cui legenda è la seguente:

- R** – Riservatezza
- I** – Integrità
- D** – Disponibilità

- A** – Ambientali
- L** – Legali

Definizioni della nomenclatura utilizzata

- Minaccia : potenziale evento dannoso
- Impatto : danno provocato da un evento dannoso
- Probabilità : probabilità di accadimento dell'evento dannoso
- Gravità : misura del danno provocato dall'evento dannoso.

L'impatto, la probabilità e la gravità sono stati stimati utilizzando una codifica a tre livelli :

- A** – Alto
- M** – Medio
- B** – Basso

RISCHI AMBIENTALI

Evento	Descrizione	Impatto	Probab.	Gravità	Misure
Evento sismico	Danni a edifici e locali con conseguente inagibilità e/o perdita di apparecchiature e dati	A	MB		Piano di Disaster Recovery
Esondazioni		A	M	A	
Attività pericolose nelle vicinanze del Centro Servizi		A	MB		

INTEGRITÀ' DEI DATI

	Trattamenti automatici	I	P	G	Trattamenti cartacei	I	P	G	Trattamenti verbali	I	P	G	Misure
R I S C H I A C C I D E N T A L I	<ul style="list-style-type: none"> comandi applicativi errati (a causa di applicazioni non testate in maniera sufficiente); comandi operativi errati (per sequenze non documentate o eseguite da personale non sufficientemente addestrato); malfunzionamenti hardware (es: guasto delle testine di un pacco di dischi); deterioramento nel tempo dei supporti di memorizzazione e del mezzo fisico che li ospita; software pericoloso, in particolare virus dei computer o utilizzo di routine tipo "superzap"; manca o interruzione di alimentazione elettrica, dovuta a black-out del fornitore del servizio; eventi disastrosi che superino i livelli ipotizzati all'atto della stesura delle contromisure. 	A	B	A	<ul style="list-style-type: none"> distruzione di documentazione per : incendio, allagamento, umidità, errori umani nell'archiviazione cartacea dei documenti (scambio di referti, cartelle cliniche, etc.) modifica non volontaria di documenti non pertinenti (scambio di documenti) 	A	B	A	<ul style="list-style-type: none"> comunicazioni non supportate da documentazione oggettiva (scambio di paziente) 	A	B	A	<p>Trattamenti elettronici</p> <ul style="list-style-type: none"> Controllo delle consegne sw (test esaustivi prima della messa in esercizio) Formazione professionale agli utenti del sistema Procedure di backup Manutenzione preventiva Installazione antivirus. UPS e gruppi di continuità aggiornamento sw antivirus <p>Trattamenti cartacei</p> <ul style="list-style-type: none"> Impianto antincendio-armadi ignifughi Policy di archiviazione/reperimento documenti <p>Trattamenti verbali</p> <ul style="list-style-type: none"> Policy
		A	B	A		A	M	A					
		A	B	M		M	M						
		A	B	A			A						
		A	B	M			B						
		A	B	A			B						

INTEGRITÀ' DEI DATI

	Trattamenti automatici	I	P	G	Trattamenti cartacei	I	P	G	Trattamenti verbali	I	P	G	Misure
R I S C H I V O L O N T A R I	<ul style="list-style-type: none"> Comandi operativi pericolosi (es. cancellazioni, copie, installazioni di sw pericolosi) interventi sull'hardware (es: spegnimenti volontari delle unità di elaborazione, furti di supporti di memorizzazione); installazione di software pericoloso (sniffer, etc.) "furto di identità elettronica" modifica non autorizzata di dati e documenti 	A	B	A	<ul style="list-style-type: none"> distruzione o furto di documentazione, modifica volontaria di documentazione da parte di personale non autorizzato o per scopi non leciti 	A	B	A	<ul style="list-style-type: none"> comunicazioni carenti o erronee agli interessati e a terzi per cui esista chiaro consenso 	A	B	A	<p>Trattamenti elettronici Sistema di controllo accessi logici Aggiornamenti periodici patch di sicurezza Procedure di backup</p> <p>Trattamenti cartacei Armadi chiusi a chiave</p> <p>Trattamenti verbali policy</p>

RISERVATEZZA DEI DATI

	Trattamenti automatici	I	P	G	Trattamenti cartacei	I	P	G	Trattamenti verbali	I	P	G	Misure
A T T A C C H I I N T E R N I	<ul style="list-style-type: none"> • “profilo” di autorizzazione all’accesso non aderente al ruolo assegnato o conseguente all’attribuzione di “privilegi” di accesso eccessivi; • “inferenza”, ossia alla cattura di un campione di informazioni che, correlate tra loro, consentano di giungere alla conoscenza indiretta di dati; • utilizzo dei privilegi di “Amministratori di Sistema” per l’accesso ad archivi (su HOST auditabile); • “furto di identità elettronica” di un dipendente autorizzato all’accesso ai sistemi; • “manomissione” delle autorizzazioni da parte del personale addetto al controllo ed all’amministrazione dei profili di accesso. 	A	B	A	<ul style="list-style-type: none"> • mancata tutela, furto, smarrimento della documentazione “in uso”; (es documentazione contenente dati sensibili, lasciata in vista di eventuali terzi non autorizzati) • mancata tutela, furto, smarrimento della documentazione archiviata 	A	M	A	<ul style="list-style-type: none"> • colloqui tenuti con o in presenza di terzi non autorizzati • Tecniche di social engineering per ottenere autorizzazioni non previste (es. richiesta della password di colleghi o di informazioni per ricostruirla facilmente) 	A	B	A	<p>Trattamenti elettronici Sistema di profilazione utenti Sistema di controllo accessi logici. Sistema di autorizzazione Divieto di uso di dispositivi personali (modem, PC,...) Controllo centralizzato. Crittografia delle comunicazioni sensibili</p> <p>Trattamenti cartacei Armadi chiusi a chiave</p> <p>Trattamenti verbali Policy</p>

RISERVATEZZA DEI DATI

	Trattamenti automatici	I	P	G	Trattamenti cartacei	I	P	G	Trattamenti verbali	I	P	G	Misure
A T T A C C H I E S T E R N I	<ul style="list-style-type: none"> • accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software; • “furto di identità elettronica” di un dipendente autorizzato all’accesso remoto ai sistemi; • intercettazione di comunicazioni telematiche, • accessi tramite collegamenti alle reti (Internet ed Intranet) da parte di operatori esterni (Hackers) con intenzioni amichevoli od ostili. 	A	B	A	<ul style="list-style-type: none"> • mancata tutela, furto, smarrimento della documentazione “in uso”; • mancata tutela, furto, smarrimento della documentazione archiviata. 	A	B	A	<ul style="list-style-type: none"> • intromissione di soggetti non autorizzati in zone o locali in cui si svolgono conversazioni su informazioni riservate 	A	B	A	<p>Trattamenti elettronici Sicurezza perimetrale Sistemi di network scanning Sistema di autenticazione Sistema di autorizzazione</p> <p>Trattamenti cartacei Armadi chiusi a chiave</p> <p>Trattamenti verbali Policy</p>

DISPONIBILITA' DEI DATI

	Trattamenti automatici	I	P	G	Trattamenti cartacei	I	P	G	Trattamenti verbali	I	P	G	Misure
R I S C H I A C C D E N T A L I	<ul style="list-style-type: none"> Mancanza di alimentazione elettrica, dovuta a black-out del fornitore del servizio; 	A	B	M	<ul style="list-style-type: none"> irreperibilità della documentazione cartacea per perdita, furto a opera di terzi, distruzione, smarrimento 	A	B	A	<ul style="list-style-type: none"> indisponibilità del personale che possiede l'informazione 	M	M	M	<p>Trattamenti elettronici Procedure per attività di manutenzione delle apparecchiature. UPS, gruppi di continuità Test delle procedure primadell'installazione</p> <p>Trattamenti cartacei Armadi chiusi a chiave Razionalizzazione dei criteri di archiviazione</p> <p>Trattamenti verbali Policy</p>
	<ul style="list-style-type: none"> Problemi relativi all'hw (p.e. guasti alle unità di elaborazione, di memorizzazione o di trasmissione); 	M	M	M	<ul style="list-style-type: none"> tempi di reperimento della documentazione cartacea non congruenti con le effettive necessità di trattamento 	M	A	M	<ul style="list-style-type: none"> carenza dei flussi informativi autorizzati (l'informazione non perviene nei tempi e nei modi congruenti al trattamento per cui è stata rilevata) 	M	M	M	
	<ul style="list-style-type: none"> Anomalie in programmi che avrebbero dovuto elaborare i dati e che non hanno potuto completare la loro esecuzione (p.e. a causa di errori di procedure per input errati, o errori di implementazione); 	M	M	M									
	<ul style="list-style-type: none"> Errate azioni del personale incaricato che impediscono l'accesso alle informazioni (p.e. mancata copia di un archivio o mancato montaggio di un supporto); dimensionamento non sufficiente delle risorse tecnologiche deputate alla trasmissione ed alla memorizzazione. 	M	M	M									

DISPONIBILITA' DEI DATI

	Trattamenti automatici	I	P	G	Trattamenti cartacei	I	P	G	Trattamenti verbali	I	P	G	Misure
R I S C H I I N T E N Z I O N A L I	<ul style="list-style-type: none"> danneggiamento o manomissione delle attrezzature sia hw che sw danneggiamento o manomissione delle connessioni. 	A	B	A	<ul style="list-style-type: none"> furto da parte di personale interno della documentazione cartacea volontario danneggiamento e/o distruzione della documentazione cartacea volontario occultamento della documentazione cartacea 	A	B	A	<ul style="list-style-type: none"> rifiuto o reticenza nel comunicare l'informazione all'interessato a ad aventi diritto generica infedeltà o comunque, negligenza e/o disobbedienza del personale addetto al controllo ed alla amministrazione delle informazioni; 	M	B	M	<p>Trattamenti elettronici Sicurezza fisica dei locali che ospitano gli apparati</p> <p>Trattamenti cartacei Archivi cartacei chiusi a chiave Controllomaccessi fisici</p> <p>Trattamenti verbali Policy</p>

6.3 Misure in essere

6.3.1 Sicurezza fisica

SERVER FARM

L'**ACCESSO** indipendente alle server farm ⁴ è consentito soltanto ai dipendenti della USL che fanno capo all'UOSI. Altri soggetti (fornitori di assistenza tecnica e manutenzione) possono entrare soltanto se accompagnati. I locali si trovano in stanze chiuse a chiave e la chiave è disponibile soltanto agli autorizzati, che si impegnano a osservare le indicazioni della relativa policy.

In particolare la sala CED del quinto piano dell'attuale sede dell'UOSI (Corso Vittorio Emanuele II) è protetta da una porta metallica taglia-fiamme dotata all'interno di maniglione anti-panico.

Il locale, adiacente l'uscita d'emergenza, è dotato di **CONDIZIONAMENTO** con un sistema in doppio che garantisce la massima affidabilità.

Durante le ore lavorative il quinto piano è accessibile al pubblico, mentre nelle ore notturne (dalle 19.00 in poi) viene chiusa a chiave la porta d'accesso. Tutte le chiavi delle porte di locali ad accesso controllato sono custodite in una cassetta chiusa a chiave a sua volta conservata in una stanza la cui chiave è affidata in custodia al responsabile/facente-funzione dell'UOSI.

DOCUMENTAZIONE CARTACEA

Tutti gli archivi cartacei contenenti informazioni personali e sensibili vengono conservati in locali o in armadi chiusi a chiave.

Per la documentazione in uso, quindi esposta alla possibilità che venga letta da non autorizzati, vengono adottati appositi criteri :

- I documenti sono inseriti in cartelline che non riportano a vista dati sensibili
- La prima pagina di ogni documento non riporta dati sensibili
- Esiste una prassi per il corretto utilizzo delle comunicazioni via fax, che prevede che le macchine siano, quando possibile, collocate vicino all'interessato e comunque nella zona riservata agli incaricati. Viene raccomandata una verifica dell'effettiva presenza dell'incaricato e sconsigliato l'invio in orari non lavorativi.

6.3.2 Sicurezza logica

SICUREZZA PERIMETRALE

E' garantita da una serie di firewall in configurazione HA. Si veda l'allegato relativo alla descrizione dettagliata della configurazione di rete. Si veda la descrizione dell'architettura logica e fisica.

SISTEMA DI AUTENTICAZIONE E AUTORIZZAZIONE

Come richiesto dalla legge, esiste un sistema di autenticazione e autorizzazione per gli utenti, e un sistema di gestione dei ruoli e dei relativi profili associati.

Il sistema di profilazione degli utenti del sistema informativo ricalca la suddivisione in classi degli incaricati, che hanno diversi ruoli e quindi livelli di autorizzazioni. Questa suddivisione in classi omogenee per ruoli è riportata su una apposita banca dati aziendale (Active Directory). Questo sistema di gestione dell'autenticazione e autorizzazione è la base per i futuri sviluppi , che prevedono l'identificazione dell'utente tramite uno strumento crittografico, tipo smart card. Attualmente il 30% degli utenti ha un profilo registrato, ma si prevede che questa percentuale arrivi al 70% nel corso del 2005.

⁴ Si veda la descrizione del sistema informatico § "Architettura fisica".

In ogni caso a ogni applicativo viene associata una password conforme alle indicazioni di legge. Esistono, presso l'ufficio "Sistemi Informativi", le funzioni di :

- **"PROVISIONING"** : profilazione e assegnazione dei diritti di accesso a fronte di una nuova assunzione e/o di una collaborazione temporanea che, a qualsiasi titolo, richieda l'accesso dai locali dell'USL alle risorse del SI, internet, intranet.

Le informazioni relative all'effettivo livello di abilitazione necessario all'interessato per raggiungere l'obiettivo istituzionale a cui è stato chiamato, vengono comunicate dai responsabili delle U.O.A. interessate che, su un apposito modulo indicano le necessità specifiche di accesso alle informazioni dell'Azienda, evidenziando in chiaro :

- la motivazione
- l'obiettivo istituzionale
- la durata del contratto di collaborazione se quest'ultimo è a tempo determinato.

A seguito della creazione di una utenza, per l'accesso al dominio, viene creata una password standard limitata al "primo utilizzo", ovvero tale da consentire all'utente di accedere una prima volta al sistema o all'applicazione e dargli modo di cambiare questa password con una personale rispondente alle indicazioni definite nell'allegato B della 196/2003.

Anche l'accesso agli applicativi è consentito tramite password completamente rispondenti alle richieste della 196. In allegato la lettera che è stata inviata ai fornitori per ottenere la formale garanzia che i loro applicativi siano conformi alla 196.

"DE-PROVISIONING" : cancellazione delle utenze e delle abilitazioni assegnate in caso di cambiamento di funzioni che modifichino il profilo d'accesso o cessazione di rapporto di lavoro a qualsiasi titolo (licenziamento, pensionamento, scadenza dei termini di contratto a termine,....)

La segnalazione delle modificate situazioni lavorative o della cessazione del rapporto di lavoro viene segnalata dai responsabili delle singole UOS.

POLITICHE DI BACKUP

Per aumentare la possibilità di ripristinare i dati vitali per l'erogazione dei servizi dell'Azienda, in tempi e in modalità opportune vengono costantemente eseguite procedure di back-up dei dati secondo le seguenti linee guida :

- Ogni giorno, nelle ore notturne, viene eseguito il "full back-up" dei dati.
- Vengono salvati i soli dati residenti sui server considerati "critici" o vitali per le attività dell'Azienda. Questa scelta è stata fatta perché su queste macchine sono ospitati i Data Base istituzionali, mentre sulle rimanenti risiedono solo applicativi e file system.
- I supporti rimovibili su cui vengono archiviati i dati personali e sensibili sono conservati in armadi chiusi a chiave, non accessibili a terzi.

ANTIVIRUS

Tra le misure di sicurezza tecniche già adottate è da segnalare l'installazione diffusa e controllata di software antivirus. Tali programmi sono installati nelle stazioni di lavoro in cui vengono svolti trattamenti in rete.

È stato adottato il prodotto della TrendMicro. Dell'intera suite sono stati acquistati :

- **ServerProtect** (per windows)

Fornisce un efficace controllo antivirus di tutta la rete per i server che funzionano con i sistemi operativi Microsoft™ Windows™ 2000, Microsoft Windows NT™, and Novell™ NetWare™. Il prodotto mette a disposizione una console portatile ed intuitiva, garantisce un controllo sugli attacchi da virus, una scansione centralizzata dei virus, gli aggiornamenti dei virus pattern file, relazioni sugli eventi e configurazione antivirus.

- **OfficeScan**

È una soluzione di sicurezza **client/server** che integra le caratteristiche principali di differenti tecnologie di sicurezza. La sua console di gestione basata su web consente agli

amministratori un accesso trasparente ai computer e ai dispositivi portatili al fine di coordinare una implementazione automatica delle policies di sicurezza e degli aggiornamenti dei software. Aiuta a far rispettare le policies e a contenere le minacce giornaliere basate su file, i virus della rete, gli intrusi, spyware ed altre ancora.

- **ScanMail** (installato su ogni server che abbia un servizio di mail)
Fornisce la protezione e la rimozione in tempo reale dai virus presenti nelle e-mail e negli allegati di posta, prima che questi possano raggiungere il desktop. Gli amministratori hanno a disposizione una console Web o Windows per configurare e gestire contemporaneamente più server Exchange e mandare notifiche agli utenti. E' un potente filtro dei contenuti progettato al fine di proteggere l'integrità dell'azienda. È completamente integrato con le più recenti API di Microsoft (AVAPI 2.0 / 2.5) Interscan virus wall.

PROTEZIONE DELLA SESSIONE DI LAVORO

Le sessioni di lavoro, una volta aperte, sono protette dall'intrusione mediante utilizzo di screen saver ad attivazione automatica.

Il periodo di attesa per l'attivazione non è modificabile da parte dell'utente, ma solo da parte degli addetti dell'Ufficio Sistemi Informativi.

RIUTILIZZO CONTROLLATO DEI SUPPORTI IN AMBIENTE PC

Esiste una prassi secondo la quale, prima della dismissione di ogni PC, ne viene completamente formattato l'hard disk, in modo irreversibile. La completa formattazione dell'hard disk viene eseguita anche nel caso in cui un PC contenente dati "sensibili" o comunque "critici" venga riassegnato da un ufficio ad un altro all'interno dell'azienda.

6.3.3 Sicurezza organizzativa

Divieto di utilizzare software non ufficialmente rilasciato dall'Azienda e preventivamente testato nella sua integrità. Tale norma assicura, peraltro, il rispetto dei contenuti del d.lgs. 518/1992 e modificazioni successive sul diritto d'autore e la tutela legale del software.

6.4 Misure da adottare

In questo paragrafo vengono descritte le misure che l'Azienda si propone di adottare nel corso del prossimo anno, prima della redazione del nuovo Documento Programmatico della Sicurezza.

6.4.1 Introduzione della Smart Card

Nel 2005 è iniziata una sperimentazione che prevede l'adozione di dispositivi crittografici per l'autenticazione forte. A questo scopo è stato pianificato e finanziato l'acquisto di 5000 smart card e di circa 1000 tastiere con lettore integrato per le postazioni di lavoro utente. I dispositivi prescelti (token Siemens) sono provvisti sia di banda magnetica che di chip crittografico. In questo modo è possibile assicurare funzioni di identificazione nel controllo accessi fisici (varchi, porte) e di autenticazione/autorizzazione logica.

Con le smart card verranno realizzate diverse funzioni di tipo crittografico quali, ad esempio la firma digitale, la crittografia dei dati, ecc.

La stessa carta verrà utilizzata per implementare e abilitare altre funzioni quali :

- Controllo accessi (fisici e logici)
- Rilevazione presenze
- Addebiti di servizi quali mensa e parcheggio,
- Ecc.

6.4.2 *Sicurezza fisica*

Nel corso del 2005 è previsto il trasferimento della server farm dalla sala attuale al 5° piano di Corso Vittorio Emanuele II, ad una sala macchine sita al primo piano dell'edificio ospedaliero di via Campagna, in una zona non esposta rischio di allagamento

L'accesso ai locali, consentito ai soli dipendenti dell'UOSI, sarà autorizzato soltanto tramite utilizzo di badge con riconoscimento biometrico e smart card.

6.4.3 *Revisione del sistema di autenticazione/autorizzazione*

E' previsto che nel corso del 2005, tutti i fornitori di sw allineeranno la gestione delle password d'accesso ai loro applicativi a quanto richiesto dalla legge. Stessa cosa faranno i fornitori di Data Base per quanto riguarda l'identificazione e la tracciatura degli accessi ai dati personali e sensibili.

L'Amministrazione provvederà a verificare l'efficacia dell'attuale profilazione utente su Active Directory per integrare e coordinare le politiche di autorizzazione con quanto implementato operativamente. In quest'ottica è prevista l'introduzione di funzionalità di autenticazione forte tramite l'utilizzo di certificati sulla smartcard.

6.4.4 *Revisione delle politiche di back-up*

Nel corso del 2005 si prevede una revisione delle politiche di back-up che potrebbe portare all'aggiornamento e miglioramento delle politiche attuali. Ad esempio si può prevedere che, per ogni server, sia pianificata un'operazione di salvataggio dell'immagine completa dei dischi (configurazioni, applicativi, customizzazioni,...), in modo da poter garantire, dopo eventuali incidenti, tempi di ripristino più ridotti rispetto agli attuali.

6.4.5 *Evoluzione del sistema di refertazione*

Nel corso del 2005 è prevista l'evoluzione del sistema di refertazione delle analisi effettuate all'interno degli Ospedali gestiti dalla AUSL. La stampa delle etichette con codice a barre sarà estesa anche ad altre tipologie di analisi cliniche (non solo quelle del sangue) e alla richiesta di visite, consulti, consulenze. Anche l'esito di queste prestazioni verrà reso automaticamente disponibile al solo personale paramedico del reparto richiedente.

E' prevista inoltre l'introduzione della **FIRMA DIGITALE** che consentirà di ridurre notevolmente la gestione dei referti cartacei, pur ottemperando alle esigenze legali di certezza di autenticità.

6.5 Piano delle attività

Le attività al momento previste per il 2005 sono :

- Introduzione della Smart Card
- Revisione del sistema di autenticazione e autorizzazione
- Introduzione della firma digitale nella refertazione.
- Nuovo CED di Piacenza
- Revisione politiche di back-up

Si è data priorità alla sperimentazione dell'introduzione della smart card come strumento in grado di migliorare il sistema di autenticazione/autorizzazione attualmente realizzato tramite "user-ID e password".

A seguire verrà sperimentato l'inserimento della firma digitale nei programmi di refertazione, questo garantirà l'autenticità del documento elettronico e la sua non modificabilità nel tempo, eliminando la fase di produzione di referti cartacei, a oggi indispensabile per ottemperare alle richieste di legge che prevedono la firma.

Sono già iniziate le attività relative alla preparazione dell'infrastruttura fisica che dovrà ospitare la server farm e gli uffici dell'UOSI di Piacenza. Si sono completati i lavori di attrezzaggio del CED, compresi l'approntamento del pavimento flottante e degli impianti di condizionamento e anti-incendio. Si sta provvedendo all'installazione dei sistemi di controllo accessi fisici. Il trasloco è previsto entro il primo semestre dell'anno in corso.

Il responsabile dell'UOSI sta identificando le figure professionali da inserire nel gruppo di lavoro che analizzerà le attuali procedure di back-up, per eventualmente progettare nuove linee guida.

Il presente piano verrà in ogni caso rivisto entro il corrente anno. Il responsabile dell'UOSI si incaricherà di verificare l'effettiva esecuzione delle attività e del livello di raggiungimento degli obiettivi iniziali.

7. FORMAZIONE / INFORMAZIONE

7.1 Attività già effettuate

Nel corso del 2004 è stato erogato un corso sui contenuti e sul significato del DL 196/2003 ai referenti indicati da ciascuna U.O.A. Questi ultimi hanno il compito di sensibilizzare direttamente i loro colleghi sui temi trattati. Presso l'Unità Operativa "Affari legali e generali" (dott.ssa Fogliazza) è disponibile la documentazione relativa al corso citato.

7.2 Attività previste

7.2.1 Formazione di base

Nel corso del 2005 sono previste iniziative di formazione sui temi della 196, diversificate per categoria d'utenza, in modo da affrontare, per ogni situazione specifica, le particolari problematiche. Il piano di formazione impostato è stato progettato con l'obiettivo di informare gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

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 previsti sono:

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

7.2.2 Formazione specifica

Nel corso del 2005 è prevista formazione specifica sull'utilizzo della smart card. La pianificazione seguirà l'iter di introduzione dello strumento nelle diverse aree organizzative. L'Ufficio gestione del personale è incaricato di verificare costantemente l'effettivo svolgimento dei predetti piani.

7.2.3 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 l'Unità Operativa Affari Generali e Legali ha deciso di attuare una politica capillare d'informazione sui temi della legge 196 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.

7.2.4 Pubblicazione sulla intranet

Sulla intranet aziendale sarà pubblicata una informativa generale riguardante gli obiettivi e i contenuti del DL 196/2003. Questo strumento è stato ritenuto di generale fruibilità e l'Unità Operativa "Marketing e comunicazione" sta studiando la forma più efficace per ottenere la miglior comunicazione.

8. ELENCO ALLEGATI

	Descrizione	Disponibile presso
All. 1	Notifica al Garante	U.O. Affari Generali e Legali Dott.ssa Fogliazza
All. 2	Elenco dei Responsabili	U.O. Affari Generali e Legali Dott.ssa Fogliazza
All. 3	Lettere d'incarico a Responsabili dei trattamenti	U.O. Affari Generali e Legali Dott.ssa Fogliazza
All. 4	Informativa agli incaricati dei trattamenti	U.O. Affari Generali e Legali Dott.ssa Fogliazza
All. 5	Lettera ai fornitori di sw Si richiede l'adeguamento alle misure minime di sicurezza previste dal DL 196/2003 in termini di password di accesso e di separazioni tra dati anagrafici e sensibili	
All. 6	Lista dei referenti delle U.O.A. per la informazione/sensibilizzazione degli incaricati	U.O. Affari Generali e Legali Dott.ssa Fogliazza
All. 7	Netviz : Mappatura fisica delle infrastrutture	U.O. Sistemi Informativi Daniele Tinelli
All. 8	Elenco Unità Organizzative	U.O. Affari Generali e Legali Dott.ssa Fogliazza
All. 9	Codice di comportamento	Gazzetta Ufficiale
All.10	Classificazione sismica dei comuni dell'Emilia Romagna	U.O. Sistemi Informativi Daniele Tinelli

Ufficio Acquisti

_____, li _____

Oggetto: richiesta di adeguamento alla normativa in tema di protezione dei dati sensibili e personali (D.L. 196/2003) del sw fornito dalla Vostra azienda alla AUSL di Piacenza

In qualità di "Titolare del Trattamento" dei dati personali, conformemente a quanto stabilito dal "Codice in materia di protezione dei dati personali" Decreto Legislativo 30 giugno 2003, n. 196 richiedo che forniate alla AUSL di Piacenza formale dichiarazione che i prodotti da Voi forniti e attualmente in uso presso la nostra Amministrazione siano conformi alle indicazioni tecniche espressamente riportate nella norma in oggetto e nel relativo allegato B.

Nello specifico :

- *La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito;*
- *la parola chiave è modificata almeno ogni tre mesi*
- *I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità*
- *I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.*
- *I dati idonei a rivelare lo stato di salute non possono essere diffusi.*

Nel caso i Vostri prodotti non dovessero essere conformi a quanto richiesto, con la presente Vi invitiamo a garantire formalmente che tutte le modifiche del caso verranno realizzate e implementate sui nostri sistemi entro e non oltre i termini previsti dalla legge.

Allo scopo di ottenere evidenza Vi invitiamo a rinviarci copia della presente firmata e compilata in ogni sua parte.

1 Nome applicativo fornito	2 Conforme		3 Sito presso il quale è installato	4 Data entro cui verrà garantita la funzionalità dell'applicativo conforme	5 Firma del legale rappresentante
	SI	NO			

La colonna 3 può riferirsi a diverse istanze dello stesso applicativo.

La colonna 4 deve essere compilata, per ogni stanza dell'applicativo specificato in colonna 1, solo nel caso in cui la versione installata e funzionante presso l'AUSL di Piacenza non sia già conforme.

La colonna 5 deve essere sempre firmata.

Il Responsabile dichiara di essere a conoscenza di quanto stabilito dal D.Lgs. 196/2003 e si impegna a adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Titolare del trattamento
Azienda USL di Piacenza nella persona di
Nome Cognome