AZIENDA SANITARIA LOCALE AL

Sede legale: V.le Giolitti, 2 – 15033 Casale Monferrato (AL)

D.L.vo 30 giugno 2003, n. 196

Documento Programmatico sulla Sicurezza

Rev. n°	*Descrizione della modifica*	*Data emissione*
00	Del. 896 del 30/03/2009	Mar. 2009
01	Del. 409 del 26/03/2010	Mar. 2010
02	Del. 243 del 25/03/2011	Mar. 2011

Indice

1. Introduzione

L'art. 34 del D.L.vo n. 196/2003 – Codice in materia di protezione dei dati personali, prescrive una serie di "misure minime di sicurezza" da adottare nel caso di trattamento di dati personali effettuato con strumenti elettronici.
Tra queste misure minime, particolare importanza riveste il Documento Programmatico sulla Sicurezza, di seguito denominato DPS.
Il citato Documento è un manuale di pianificazione della sicurezza dei dati che attesta l'adeguamento dell'Azienda alla normativa a tutela del patrimonio informativo in essere, intendendosi per tale sia quello custodito in banche dati informatizzate, sia quello custodito nei tradizionali archivi cartacei.
Con il DPS l'Azienda intende descrivere la situazione attuale, attraverso l'analisi dei rischi, la distribuzione dei compiti, le misure approntate e la distribuzione delle responsabilità, nonché il percorso di adeguamento prescelto per adeguarsi alle prescrizioni del Codice.
Gli obiettivi indicati sono perseguiti dando conto di una serie di informazioni il cui contenuto è esplicitato nella Regola 19 del Disciplinare Tecnico in materia di misure minime di sicurezza, allegato B al Codice.

La Regola anzidetta si articola nei seguenti 8 punti:
19.1 l'elenco dei trattamenti di dati personali.
19.2 la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati, nonché alle responsabilità gestionali dei Dirigenti.
19.3 l'analisi dei rischi che incombono sui dati, finalizzata alla tutela dei dati personali; questa analisi permette di individuare le priorità di intervento e le conseguenti necessarie misure di sicurezza.
19.4 le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità; questo elenco deve essere il risultato dell'analisi dei rischi e deve garantire sia la sicurezza (intesa come riservatezza, integrità e disponibilità) dei dati personali, sia quella delle strutture fisiche in cui i dati sono custoditi (PC, locali, altro).
19.5 la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento degli stessi o degli strumenti elettronici, in tempi certi e compatibili con i diritti degli interessati; in questa parte è importante prevedere il salvataggio di tutti i dati personali contenuti nelle banche dati dell'Azienda, controllare l'effettivo esito positivo delle operazioni di salvataggio, prevedere la possibilità di ricostruire l'intero sistema operativo ed i programmi applicativi.
19.6 la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.
19.7 la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno dell'Azienda.
19.8 per i dati personali idonei a rivelare lo stato di salute e la vita sessuale trattati dagli Organismi Sanitari e dagli esercenti le professioni sanitarie, devono essere individuati dei criteri da adottare per la cifrature o per la separazione di tali dati dagli altri dati personali dell'interessato.

Questa Azienda procederà all'aggiornamento annuale del DPS, così come stabilito dall'art. 34, comma 1, lettera g) del D.Lgs. 196/2003 e dal punto 19 dell'allegato B del Codice stesso.

1.1 Oggetto e scopo del documento

Il presente DPS è redatto per soddisfare tutte le misure minime di sicurezza che debbono essere adottate in via preventiva da tutti coloro che trattano dati personali, conformemente a quanto previsto dal Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003).
Inoltre costituisce un valido strumento per l'adozione delle misure previste dall'art. 31, dall'art. 34 e dall'art. 35 dello stesso Codice e dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del D.Lgs. 196/2003).
Scopo del presente DPS è quello di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

1.2. Campo di applicazione

Il Documento Programmatico Sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.
Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Il Documento Programmatico Sulla Sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

2. Elenco trattamenti dei dati personali
(Regola 19 punto 19.1)

2.1. Finalità del trattamento dei dati
Viene riportato in questa sezione l'elenco dei trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati trattati e della struttura interna od esterna che operativamente effettua il trattamento. Per ogni trattamento è specificato dove sono ubicate le banche dati e la tipologia di accesso ed interconnessione.

2.2. Elenco dei trattamenti censiti
Nella tabella 1 e 2 è riportato l'elenco dei trattamenti censiti con indicazione in particolare:

- *Descrizione sintetica*: descrizione del trattamento dei dati personali attraverso l'indicazione della finalità perseguita e delle categorie di persone cui i dati si riferiscono.
- *Natura dei dati trattati*: indicazione se, tra i dati personali, sono presenti dati sensibili o giudiziari.
- *Struttura di riferimento*: indica la struttura all'interno della quale viene effettuato il trattamento.
- *Altre strutture che concorrono al trattamento*: nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture vengono indicate, oltre a quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.
- *Descrizione degli strumenti elettronici utilizzati:* indica la tipologia di strumenti elettronici impiegati.
- *Banca Dati*: indica la banca dati (ovvero il data base o l'archivio informatico), con le relative applicazioni, in cui sono contenuti i dati.
- *Ubicazione dei supporti di memorizzazione*: indica il luogo in cui risiedono fisicamente i dati, ovvero dove si trovano gli elaboratori sui cui dischi sono memorizzati i dati, i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza ed ogni altro supporto rimovibile.
- *Tipologia dei dispositivi*: elenco e descrizione sintetica degli strumenti utilizzati dagli incaricati per effettuare il trattamento: pc, terminale non intelligente, palmare, telefonino, ecc.
- *Connessione*: descrizione sintetica e qualitativa della rete che collega i dispositivi d'accesso ai dati utilizzati dagli incaricati: rete locale, geografica, Internet, ecc.

Tab. 1.1 – Elenco trattamenti: informazioni essenziali

Descrizione sintetica del trattamento		***Natura dei dati trattati***		***Struttura di riferimento***	***Altre strutture che concorrono al trattamento***	***Descrizione degli strumenti utilizzati***
Finalità perseguite	***Categorie di interessati***	***Sensibili***	***Giudiziari***			
Assistenza Sanitaria; Gestione Amministrativa; Indagine Epidemiologica; Monitoraggio della spesa sanitaria; Analisi dei flussi di mobilità sanitaria attiva e passiva; Analisi dell'andamento della domanda e dell'offerta sanitaria	Assistiti; Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione; Deceduti; Donatori o Riceventi; Malati gravi o sottoposti a particolari trattamenti di cura; Neonati; Pazienti; Assistiti di altre AA.SS.LL:	X		SOC Programmazione e Controllo di Gestione	Altre Strutture Aziendali IG Consulting-Modena	PC
Attività di Segreteria e Protocollo; Gestione di rapporti di lavoro e collaborazioni varie.	Amministratori, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo; Cittadini di paesi appartenenti all'UE; Cittadini italiani; Clienti o utenti; Imprenditori individuali, piccoli imprenditori o liberi professionisti; Lavoratori o collaboratori; Persone fisiche; Persone in cerca di occupazione.			SOC Programmazione Strategica e Affari Generali		PC
Erogazione competenze mensili ai dipendenti; Liquidazione compenso per titolari di incarichi e collaborazioni; Rilascio CUD; Effettuazione trattenute di legge; Gestione politiche del personale; Formazione professionale.	Personale dipendente; Titolari di contratti di collaborazione coordinata e continuativa; Borsisti; Tirocinanti disabili; Libero professionisti; Specialisti ambulatoriali; Cittadini di paesi appartenenti alla U.E.; Cittadini italiani; Lavoratori o collaboratori; Persone fisiche; Persone in cerca di occupazione.	X	X	SOC Personale	Altre Strutture Aziendali.	PC
Affitti attivi e passivi; Alienazioni di beni patrimoniali; Gestione patrimonio mobiliare i immobiliare; Anagrafi clienti e fornitori; Fatturazione attiva di prestazioni sanitarie istituzionali e di libera professione; Interrogazione banche dati Equitalia/Enti	Amministratori, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo; Cittadini italiani; Persone fisiche; Persone giuridiche ed altri enti; Imprenditori individuali, piccoli imprenditori o liberi		X	SOC Economico Finanziario e Patrimoniale	Altre strutture Aziendali.	PC

previdenziali e Assicurativi; Cessioni quinto stipendio/ ritenute sindacali/pignoramenti stipendi.	professionisti; Clienti o utenti; Lavoratori o collaboratori.					
Lavori Pubblici	Amministratori, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo; Imprenditori individuali, piccoli imprenditori o liberi professionisti; Persone fisiche; Persone giuridiche ed altri enti.		X	SOC Tecnico		PC
Fornitura di beni o servizi; Attività commerciali.	Ditte partecipanti a gare d'appalto		X	SOC Logistica Economato		PC
Acquisizione beni e servizi; attività commerciali.	Amministratori, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo; Imprenditori individuali, piccoli imprenditori o liberi professionisti; Persone fisiche; Persone giuridiche ed altri enti		X	SOC Provveditorato		PC
Attività connesse al settore assicurativo; Attività connesse al contenzioso amministrativo; Attività connesse al recupero crediti; Fornitura di beni o servizi; Attività commerciali; Prevenzione, accertamento e repressione di reati.	Amministratoti, coordinatori o altre persone che ricoprono incarichi in organismi di tipo associativo; Cittadini di paesi appartenenti all'UE; Cittadini di paesi non appartenenti all'UE; Cittadini italiani; Clienti o utenti; Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione; Deceduti; Imprenditori individuali, piccoli imprenditori o liberi professionisti; Indagati o imputati; Lavoratori o collaboratori; Parenti, affini o conviventi; Persone fisiche; Persone giuridiche ed altri enti; Scolari o studenti di ogni ordine e grado; Soci, associati, aderenti o iscritti.	X	X	Ufficio Legale	Altre Strutture Aziendali; Equitalia; Compagnie Assicurative; Professionisti; Autorità Giudiziaria; Enti Locali; C.C.I.A.A.;	PC
Assistenza Sanitaria; Diagnosi, cura o	Assistiti; Deceduti; Lavoratori o					

terapia dei pazienti; Gestione amministrativa; Registrazione dei pazienti; Rilevazione di malattie infettive e diffusive; Rilevazione di stati di sieropositività; Schede cliniche informatizzate; Attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione; Programmazione, gestione, controllo e valutazione dell'assistenza sanitaria; Instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il SSN; Interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza domiciliare.	collaboratori; Personale dipendente.	X		SOC Sistemi Informatici	Sas Institute s.r.l.; Cleis Tech s.r.l.; Ig Consulting s.r.l.; Biosoft s.r.l.; Italcom S.p.A.; Lantech Solutions s.r.l.; Eurosoft Informatica Medica s.r.l.; Laboratorio di Informatica Medica s.r.l.; Sowre s.r.l.; Netribe s.r.l.; Honeywell s.r.l.; Siemens S.p.A.; Metafora Informatica s.r.l.; Fas s.r.l.; Cabril Service s.r.l.; Ditelo sas; IBM Italia S.p.A.; Agfa Fuji.	PC
Prevenzione di determinate patologie; Programmi terapeutici o di prevenzione; Prevenzione malattie professionali.	Gruppi omogenei per fattori di rischio; Lavoratori o collaboratori; Maggiori di età; Personale dipendente.	X		Medico Competente	Altre Strutture aziendali.	PC
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; Prevenzione e diagnosi di Patologie descritte nel registro nazionale delle malattie rare; Perizie medico-legali; diagnosi e screening prenatali; Trapianti di organi e tessuti; Assistenza Sanitaria; Diagnosi dei pazienti; Gestione Amministrativa; Indagine epidemiologica; Interventi in caso di calamità, epidemie o malattie infettive; Monitoraggio della spesa sanitaria;	Concepiti e nascituri; Coniugi e conviventi; Deceduti; Persone disabili; Genitori; Gruppi omogenei per abitudini sessuali, appartenenza razziale o etnica, area geografica, caratteristiche fisiche, consanguineità, fattori di rischio; Lavoratori o collaboratori; Persone affette; Minori; Parenti, affini o conviventi; Soggetti con limitata capacità di intendere e volere; Assistiti; Donatori o riceventi; Malati gravi o sottoposti a particolari trattamenti di cura; Neonati; Maggiori di età; Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione; Gruppi familiari; Indagati o imputati; Pazienti; Personale	X	X	Distretti	Altre Strutture Aziendali; Cooperativa BIOS e SCATA; ARTSANA; Ferrero Service; Convatec; Johnson; Vivisol s.r.l.; Officina Ortopedica s.r.l.; Medinord s.r.l.; Sanix International S.p.A.; Medical A.R.S.; Medic AIR s.r.l.; Sapio Life s.r.l.; Vital Aire s.r.l.; Baxter; Laboratori Odontotecnici; CRI e altre Associazioni di trasporto autorizzate; Scuole di ogni ordine e grado; A.S.C.A. (Associazione	PC

Prevenzione di patologie genetiche in popolazioni a rischio; Prenotazione e refertazione di esami clinici o visite specialistiche per via telematica o telefonica; Prestazione di servizi sanitari relativi a banche di dati o alla fornitura di beni; Procreazione assistita; Registrazione dei pazienti; Rilevazione di malattie infettive e diffusive, mentali e di stati di sieropositività; Schede cliniche informatizzate; Attività di previdenza; Fornitura di beni e servizi; Identificazione individuale su tracce biologiche; Ricerca medica o biomedica; Ricerca statistica; Ricerca storica; Sperimentazioni farmacologiche ad uso clinico; Attività di teleconsulto, telediagnosi o telemedicina; Prescrizione elettronica dei farmaci.	dipendente; Scolari o studenti di ogni ordine e grado.				socio assistenziale dei comuni dell'Acquese – Comunità montana Suol Aleramo); MARCONDIRO COOP; Consorzio Servizi alla persona – Novi Ligure.	
Prevenzione di determinate patologie; Cura e terapia degli interessati; Cura e terapia dei familiari dell'interessato; Diagnosi delle patologie genetiche; Diagnosi di Patologie descritte nel registro nazionale delle malattie rare; Diagnosi prenatali; Mappatura genetica; Prevenzione di patologie descritte nel registro nazionale delle malattie rare e/o in quelle regionali; Ricerca medica o biomedica; Ricerca statistica; Ricerca storica; Screening neonatali; Sperimentazioni farmacologiche ad uso clinico; Trapianti di organi e tessuti; Altre forme di sicurezza privata; Controllo di particolari aree o strumenti per fini di tutela di beni o persone; Assistenza sanitaria; Attività di	Concepiti e nascituri; Coniugi e conviventi; Genitori; Addetti alla sicurezza; Clienti o utenti; Lavoratori o collaboratori; Minori di età; Passeggeri su veicoli o utenti di mezzi di trasporto; Pazienti, degenti o disabili; Assistiti; Deceduti; Donatori o riceventi; Gruppi familiari; Maggiori di età; Malati gravi o sottoposti a particolari trattamenti di cura; Neonati; Pazienti; Personale dipendente; Parenti, affini o conviventi; Persone fisiche; Soggetti con limitata capacità di intendere e volere; Gruppi omogenei per caratteristiche fisiche; Gruppi omogenei per consanguineità; Gruppi omogenei per fattori di rischio; Gruppi omogenei per abitudini sessuali; Gruppi omogenei per nazionalità; Gruppi	X	X	Presidi Ospedalieri	Altre Strutture Aziendali; Altre AA.SS.LL. e AA.SS.OO. regionali ed extraregionali; Case di Cura accreditate; ECORAD ATP; Laboratorio Toma; Società Alliance Medical S.r.l.;	PC

teleconsulto, telediagnosi e telemedicina; Diagnosi, cura e 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; Rilevazione di malattie infettive e diffusive; Rilevazione di malattie mentali; Rilevazione di stati di sieropositività; Schede cliniche informatizzate; Prevenzione, accertamento e repressione di reati; Prevenzione; Identificazione su tracce biologiche; Cura e terapia di terzi; Programmi terapeutici o di prevenzione; Perizie medico – legali; Prestazione di servizi sanitari relativi a banche di dati o alla fornitura di beni.	omogenei per provenienza geografica; Scolari o studenti di ogni ordine e grado; Gruppi omogenei per altre caratteristiche.					
Sorveglianza sanitaria per la tutela della salute pubblica; Indagine epidemiologica; Interventi in caso di calamità, epidemie o malattie infettive; Prevenzione; Ricerca medica e biomedica; Rilevazione di malattie infettive o diffusive; Prevenzione infortuni; Tutela salute e sicurezza dei lavoratori; Analisi dell'uso di merce in distribuzione o in commercio; Difesa del suolo, igiene urbana o tutela dell'ambiente; Prevenzione, accertamento e repressione di reati; Mappatura delle strutture in cui sono	Adulti; Bambini; Italiani; Stranieri; Lavoratori e utenti; Cittadini UE; Clienti o utenti; Persone che possono contrarre malattie trasmesse da animali o prodotti di origine animale; Imprenditori individuali, piccoli imprenditori o liberi professionisti; Persone giuridiche ed altri enti; Allevamenti che utilizzano prodotti di cui all'art. 1 del Reg. Ce n. 79/2005.	X	X	Dipartimento di Prevenzione	Regione Piemonte; Amministrazioni Locali varie; Servizi Veterinari delle AA.SS.LL. Piemontesi; Veterinari libero professionisti; Ministero della Sanità e dell'Agricoltura; Ditta Ecorad; Procura della Repubblica; NAS; CSI; INAIL; Autorità Giudiziaria; Direzione Provinciale del Lavoro; ARPA Piemonte; Clinica del Lavoro	PC

detenuti animali; Vigilanza sul commercio di animali; Aggiornamento delle anagrafi zootecniche.					Università di Milano.	
Assistenza Sanitaria; Diagnosi, cura o terapia dei pazienti; Monitoraggio della spesa sanitaria; Registrazione dei pazienti; Rilevazione malattie mentali; Servizi sociali; Ricerca scientifica: Interventi sanitari o socio sanitari ad alta integrazione; Attività di teleconsulto; Prescrizione elettronica dei farmaci; Registrazione dei pazienti; Ricerca medica o biomedica; Schede cliniche informatizzate.	Assistiti; Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione; Malati gravi o sottoposti a particolari trattamenti di cura; Pazienti; Soggetti con limitata capacità di intendere e volere; Pazienti affetti da patologie psichiatriche; Maggiori di età; Cittadini appartenenti e non all'UE; Clienti o utenti; Persone disabili.	X	X	Dipartimento di Salute Mentale		PC
Assistenza Sanitaria; Trapianto di organi e tessuti; Diagnosi, cura o terapia dei pazienti; Gestione Amministrativa; Indagine epidemiologica; Monitoraggio della spesa sanitaria; Prestazione di servizi sanitari relativi a banche di dati o alla fornitura di beni; Procreazione assistita; Registrazione dei pazienti; Schede cliniche informatizzate.	Assistiti; Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione; Deceduti; Donatori o riceventi; Lavoratori o collaboratori; Maggiori di età; Malati gravi o sottoposti a particolari trattamenti di cura; Minori di età; Neonati; Pazienti; Personale dipendente; Soggetti con limitata capacità di intendere e di volere.	X		Dipartimento del Farmaco		PC
Assistenza Sanitaria; Diagnosi, cura o terapia dei pazienti; Gestione Amministrativa; Indagine epidemiologica; Monitoraggio della spesa sanitaria; Prenotazione e refertazione di esami clinici o visite specialistiche per via telematica o telefonica; Prescrizione elettronica dei farmaci; Prestazione di servizi sanitari relativi a banche dati o alla fornitura di beni; Registrazione dei pazienti; Ricerca medica o biomedica;	Assistiti; Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione; Deceduti; Genitori; Gruppi familiari; Indagati o imputati; Lavoratori e collaboratori; Maggiori di età; Minori di età; Malati gravi o sottoposti a particolari trattamenti di cura; Neonati entro il primo anno di vita; Parenti, affini o conviventi; Pazienti; Soggetti con limitata capacità di intendere e di volere; Utenti o clienti; Consumatori; Persone disabili; Persone affette; Militari o appartenenti alle forze dell'ordine;	X	X	Dipartimento delle Dipendenze		PC

Rilevazione di malattie infettive e diffusive; Rilevazione di malattie mentali; Rilevazione di stati di sieropositività; Schede cliniche informatizzate; Servizi sociali; Ricerca statistica e scientifica; Creazione di profili professionali relativi a clienti o consumatori; Attività informativa; Attività amministrativa o giudiziaria; Analisi delle abitudini o scelte di consumo.	Scolari di ogni ordine e grado; Soggetti in difficoltà o pericolo.					
Identificazione individuale su tracce biologiche; Diagnosi delle patologie genetiche; Diagnosi di patologie descritte nel registro nazionale delle malattie rare; Perizie medico legali; Ricerca medica o biomedica; Ricerca statistica; Ricerca storica; Accertamento stato invalidità civile, cecità, sordomutismo, handicap; Per relazioni su cause relative a decessi richieste dall'autorità giudiziaria; Esenzioni ticket per patologia; Assistenza sanitaria; Legge 210/1992.	Concepiti e nascituri; Coniuge e conviventi; Deceduti; Persone disabili; Genitori; Gruppi omogenei per abitudini sessuali; Gruppi omogenei per appartenenza razziale o etnica; Gruppi omogenei per area geografica; Gruppi omogenei per caratteristiche fisiche; Gruppi omogenei per consanguineità; Gruppi omogenei per fattori di rischio; Lavoratori o collaboratori; Maggiori di età; Persone affette; Minori di età; Parenti, affini o conviventi; Soggetti con limitata capacità di intendere e volere.	X	X	SOC Medicina Legale		PC
Assistenza sanitaria sociale; Diagnosi, cura o terapia dei pazienti; Gestione amministrativa; Indagine epidemiologica; Interventi in caso di calamità, epidemie o malattie infettive; Monitoraggio della spesa sanitaria-sociale; Registrazione dei pazienti; Rilevazione di malattie mentali.	Assistiti; Concepiti e nascituri; Condannati, deceduti o sottoposti a misure di sicurezza o prevenzione; Deceduti; Genitori; Gruppi familiari; Gruppi omogenei per caratteristiche fisiche; Gruppi omogenei per nazionalità; Indagati o imputati; Lavoratori o collaboratori; Maggiori di età; Malati gravi o sottoposti a particolari trattamenti di cura; Minori di età; Neonati; Parenti, affini o conviventi; Pazienti; Scolari o studenti di ogni ordine e grado; Soggetti con limitata capacità di intendere e volere.	X		Direzione Socio Assistenziale Distretto di Casale	Altre Strutture Aziendali; Coop. Punto Service; Coop. Nuova Idea; Coop. Codess.	PC
Prevenzione di determinate patologie;	Concepiti e nascituri; Coniuge e conviventi; Deceduti; Persone					

Programmi terapeutici o di prevenzione; Perizie medico legali; Prevenzione di patologie descritte nel registro nazionale delle malattie rare e/o in quelli regionali; Ricerca statistica; Gestione amministrativa.	disabili; Genitori; Gruppi omogenei per fattori di rischio; Lavoratori o collaboratori; Maggiori di età; Soggetti con limitata capacità di intendere e volere; Indagati o imputati; Malati gravi o sottoposti a particolari trattamenti di cura; Personale dipendente.	X	X	SOC Coordinamento SITRO		PC
Mappatura della realtà all'interno degli Istituti Penitenziari; Diagnosi, cura o terapia dei pazienti detenuti; Indagine epidemiologica; interventi in caso di malattie infettive; Monitoraggio della spesa sanitaria; Rilevazione di: malattie infettive, malattie mentali e stati di sieropositività.	Condannati, detenuti o sottoposti a misure di sicurezza o prevenzione; Indagati, imputati, collaboratori di giustizia, detenuti in regime di elevato indice di sorveglianza e altri regimi speciali di detenzione.	X	X	SOC Servizio Tutela della Salute in Carcere	Soggetti privati; Soggetti pubblici; Organismi del SSN; Autorità giudiziaria e penitenziaria.	PC
Finalità dell'ufficio	Clienti o utenti; Personale dipendente		X	Business Unit Libera Professione	Altre strutture aziendali; Cliniche private.	PC

Tab. 1.2 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti

Finalità perseguite	***Banca Dati***	***Ubicazione***	***Tipologia dispositivi***	***Connessione***
Assistenza Sanitaria;	UGSD00 SANITARIO UGSD00 CED LHA AURA	SC Sistema Informativo Tortona SOC Sistema Informativo Casale CSI Piemonte	PC	Rete LAN / WAN
Gestione Amministrativa;	UAM CED2	SOC Sistema Informativo Casale	PC	Rete LAN / WAN
Monitoraggio della spesa sanitaria; Analisi dei flussi di mobilità sanitaria attiva e passiva; Analisi dell'andamento della domanda e dell'offerta sanitaria	GIOVE CASSANDRA	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	PC	Rete LAN / WAN
Attività di Segreteria e Protocollo; Gestione di rapporti di lavoro e collaborazioni varie.	ATTIUNICI	SOC Sistema Informativo Casale	PC	Rete LAN / WAN
Erogazione competenze mensili ai dipendenti; Liquidazione compenso per titolari di incarichi e collaborazioni; Rilascio CUD; Effettuazione trattenute di legge; Gestione politiche del personale; Formazione professionale.	WHR	SC Sistema Informativo Tortona	PC	Rete LAN / WAN
Affitti attivi e passivi; Alienazioni di beni	UAE CED2	SOC Sistema	PC	Rete LAN / WAN

patrimoniali; Gestione patrimonio mobiliare i immobiliare; Anagrafi clienti e fornitori; Fatturazione attiva di prestazioni sanitarie istituzionali e di libera professione; Interrogazione banche dati Equitalia/Enti previdenziali e Assicurativi; Cessioni quinto stipendio/ ritenute sindacali/pignoramenti stipendi.	Archivi Informatica Individuale	Informativo Casale Altre sedi		
Attività connesse al settore assicurativo; Attività connesse al contenzioso amministrativo; Attività connesse al recupero crediti;	Archivi Informatica Individuale	S.C. Ufficio Legale, Settore Gestione Assicurazioni e Consulenza – sede di Novi Ligure, Ovada, Settore Gestione Contenzioso Amministrativo e Recupero Crediti Sede di Casale Monferrato	PC	Rete LAN / WAN
Fornitura di beni o servizi; Attività commerciali;	UAE CED2	SOC Sistema Informativo Casale	PC	Rete LAN / WAN
Schede cliniche informatizzate	MedOffice GA	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	PC	Rete LAN / WAN
Diagnosi dei pazienti strumenti radiologici	SYNAPSE	SC Sistema Informativo Tortona SOC Sistema Informativo Casale SC Informatica Novi	PC	Rete LAN / WAN
Prenotazione e refertazione di esami clinici o visite specialistiche per via telematica o telefonica	TELECUP	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	PC	Rete LAN / WAN
Diagnosi dei pazienti strumenti Laboratorio Analisi	METAFORA GELAB	SC Sistema Informativo Tortona SOC Sistema Informativo Casale SC Informatica Novi	PC	Rete LAN / WAN
Sorveglianza sanitaria per la tutela della salute pubblica; Indagine epidemiologica; Interventi in caso di calamità, epidemie o malattie infettive; Prevenzione; Ricerca medica e biomedica; Rilevazione di malattie infettive o diffusive;	EPIDEM	SC Epidemiologia	PC	Rete LAN / WAN
Prevenzione infortuni; Tutela salute e sicurezza dei lavoratori; Analisi dell'uso di merce in distribuzione o in commercio; Difesa del suolo, igiene urbana o tutela dell'ambiente; Prevenzione, accertamento e repressione di reati;	Archivi Informatica Individuale	IGIENE PUBBLICA	PC	Rete LAN / WAN
Mappatura delle strutture in cui sono detenuti animali; Vigilanza sul commercio di animali; Aggiornamento delle anagrafi zootecniche.	ARVET	SC Sistema Informativo Tortona SOC Sistema Informativo Casale SC Informatica Novi Regione Piemonte	PC	Rete LAN / WAN

Accertamento stato invalidità civile, cecità, sordomutismo, handicap; Per relazioni su cause relative a decessi richieste dall'autorità giudiziaria; Esenzioni ticket per patologia; Assistenza sanitaria; Legge 210/1992.	UGSD00 SANITARIO UGSD00 CED	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	PC	Rete LAN / WAN

3. Distribuzione dei compiti e delle responsabilità
(Regola 19 punto 19.2)

3.1. Descrizione dell'Azienda
L'Azienda ASL "AL", istituita con Decreto del Presidente della Giunta Regionale del Piemonte n. 85 del 17.12.2007, sostituisce, unificandone le competenze e le funzioni, le tre AA.SS.LL. (ASL 20, ASL 21, ASL 22) che in precedenza operavano su singole porzioni del territorio provinciale.
La missione istituzionale dell'ASL AL consiste nel farsi carico, in modo costante ed uniforme, dei bisogni di salute dei residenti e nel garantire ai predetti l'erogazione delle prestazioni inserite nei livelli essenziali di assistenza, direttamente o attraverso il ricorso a strutture esterne accreditate, pubbliche o private, assicurando risposte qualificate, appropriate e tempestive, su più livelli di complessità.

L'ASL AL ha sede legale in Viale Giolitti n. 2 – 15033 Casale Monferrato.

L'ambito territoriale dell'Azienda Sanitaria Locale AL comprende, in sintesi, le seguenti strutture:

Presidi Ospedalieri:
- Presidio Ospedaliero di Acqui Terme
- Presidio Ospedaliero di Casale Monferrato
- Presidio Ospedaliero di Novi Ligure
- Presidio Ospedaliero di Ovada
- Presidio Ospedaliero di Tortona
- Presidio Ospedaliero di Valenza

Distretti:
- Acqui Terme
- Alessandria
- Casale Monferrato
- Novi Ligure
- Ovada
- Tortona
- Valenza

Strutture Tecnico Amministrative di supporto:
- Dipartimento Amministrativo
- Dipartimento Tecnico - Logistico

Dipartimento di Prevenzione:

Il Dipartimento di prevenzione, ai sensi degli artt. 7 e ss. D.Lgs. 502/1992 e s.m.i., è una macro struttura organizzativa preposta all'attività propria del livello di assistenza sanitaria collettiva in ambiente di vita e di lavoro, attraverso l'organizzazione e la promozione della tutela della salute della popolazione mediante azioni tendenti a conoscere, prevedere e prevenire gli infortuni e le cause di malattia.

Strutture in Staff alla Direzione Generale:

- Uffici di Staff;
- Funzioni Delegate;
- Coordinamenti.

3.2 Trattamenti effettuati dall'Azienda

Con il termine "trattamento", ai sensi dell'art. 4, comma 1, lett. a) del D.Lgs. 196/2003, deve intendersi 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 dei dati.
L'ASL AL, in quanto organismo sanitario pubblico, tratta dati inerenti la salute.
Qualunque trattamento di dati personali da parte dell'ASL AL è consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18 D.Lgs. 196/2003), al fine di adempiere a compiti ad essa attribuiti da leggi e regolamenti.
E' possibile effettuare trattamenti relativi a dati diversi da quelli sensibili e giudiziari anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente, fermo restando l'esercizio di funzioni istituzionali. Il trattamento dei dati sensibili è invece consentito solo se autorizzato da espressa disposizione di legge nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.
Nei casi in cui una disposizione specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in relazione ai tipi di dati e di operazioni identificati e resi pubblici con atto di natura regolamentare di cui all'art. 20, comma 2, del D.Lgs. 196/2003.
Per descrivere sinteticamente i trattamenti effettuati dall'ASL AL, i compiti e le relative responsabilità delle Strutture, in relazione ai trattamenti effettuati, si riporta la seguente tabella.

Tab. 2 – Competenze e responsabilità delle strutture preposte ai trattamenti

Struttura	Trattamenti effettuati dalla Struttura	Descrizione sintetica dei compiti e delle responsabilità della struttura
SOC Programmazione e Controllo di Gestione	Elaborazione di dati raccolti da terzi; Organizzazione in banche dati; Raccolta di dati mediante strumenti elettronici; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Trattamenti temporanei finalizzati ad una rapida aggregazione di dati o alla loro trasformazione in forma anonima; Acquisizione dei dati dal CSI-Piemonte (da piattaforma CSI-Piemonte o da invio informatico); Gestione del dato tramite sistemi informatici aziendali (software gestionali-applicativi per la gestione della mobilità sanitaria).	Acquisizione, caricamento e consultazione dati; Acquisizione, elaborazione e consultazione dati; Memorizzazione in archivi suddivisi per tipo di informazione; Acquisizione, elaborazione ed invio dati; Elaborazione in forma aggregata di dati senza informazioni sensibili; Predisposizione reportistica in forma cartacea e su supporto elettronico.
SOC Programmazione Strategica e Affari Generali	Organizzazione in banche dati in forma prevalentemente automatizzata; Raccolta di dati presso l'interessato; Elaborazione di dati raccolti da terzi; Operazioni di trattamento affidate in parte a terzi;	Acquisizione e caricamento dati; Consultazione.

	Raccolta di dati a fini di trattamento da parte di terzi; Raccolta di dati mediante strumenti elettronici; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale	
SOC Personale	Raccolta moduli cartacei (tabulati rilevazione presenze, dichiarazione dei dipendenti per situazioni personali ai fini detrazioni fiscali – variazioni anagrafiche ecc.); Inserimento su procedure elaborazioni stipendiali; Liquidazione fatture previo inserimento in procedura ordini. Gestione del personale; Trattamento di quiescenza.	Acquisizione e caricamento dati; Consultazione; Comunicazione a terzi.
SOC Economico Finanziario e Patrimoniale	Associazione o raffronto di dati anche provenienti da diverse banche dati pubbliche o private; Raccolta di dati per via informatica o telematica; Organizzazione in banche dati in forma prevalentemente non automatizzata; Raccolta dati presso organismi e strutture del servizio sanitario nazionale; Organizzazione in banche dati in forma prevalentemente informatizzata; Raccolta presso registri, elenchi atti o documenti pubblici.	Comunicazione a terzi; Acquisizione; Caricamento dati; Salvataggio; Ripristini; Comunicazione a terzi; Consultazione riscossioni.
SOC Tecnico	Raccolta dati da professionisti per consulenze e progetti, da ditte per gare d'appalto e da Enti per verifiche; associazione o raffronto di dati anche provenienti da diverse banche dati pubbliche o private; Raccolta di dati per via informatica o telematica; Organizzazione in banche dati in forma prevalentemente non automatizzata; Raccolta dati presso organismi e strutture del servizio sanitario nazionale; Organizzazione in banche dati in forma prevalentemente informatizzata.	Comunicazione a terzi; Acquisizione; Caricamento dati; Salvataggi; Ripristini.
SOC Logistica Economato	Raccolta dati presso l'interessato; Organizzazione in banche dati in forma prevalentemente non automatizzata.	Acquisizione e caricamento dati; Consultazione; Conservazione.
SOC Provveditorato	Associazione o raffronto di dati anche provenienti da diverse banche dati pubbliche o private; Raccolta di dati per via informatica o telematica; Organizzazione in banche dati in forma prevalentemente non automatizzata; Raccolta dati presso organismi e strutture del servizio sanitario nazionale; Organizzazione in banche dati in forma prevalentemente informatizzata.	Acquisizione e caricamento dei dati; Consultazione.
Ufficio Legale	Associazione o raffronto di dati anche provenienti da diverse banche dati pubbliche o private; Organizzazione in banche dati in forma prevalentemente automatizzata; Raccolta dati per via informatica o telematica; Raccolta dati presso l'interessato; Raccolta dati presso organismi o strutture del S.S.N.; Raccolta dati presso registri, elenchi, atti o documenti pubblici; Raccolta dati presso terzi.	Acquisizione e caricamento dati; Consultazione.
SOC Sistemi Informatici	Trattamento relativo ai dati gestiti con strumenti informatici e riguardante le attività amministrative correlate all'erogazione di prestazioni sanitarie di ricovero, specialistiche, di diagnostica strumentale e di laboratorio, di riabilitazione nonché all'attività epidemiologica sistematica a supporto delle funzioni di programmazione, gestione, controllo e valutazione dell'assistenza; Collegamento dei dati idonei a rilevare lo stato di salute o la vita sessuale con informazioni relative a pagamenti, esenzioni o corretta prescrizione di medicinali; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale.	Gestione autorizzazione su applicativi; Manutenzione tecnica e gestione tecnico operativa della base dati; Comunicazione a terzi.
Medico Competente	Prevenzione di determinate patologie; Raccolta dati in cartelle cartacee; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Gestione dati sanitari.	Sorveglianza sanitaria dei lavoratori.
Distretti	Organizzazione in banche dati in forma prevalentemente automatizzata; Organizzazione in banche dati in forma prevalentemente non automatizzata; Prevenzione di determinate patologie; Raccolta di dati mediante strumenti elettronici; Raccolta di dati presso terzi; Prevenzione nelle popolazioni a rischio genetico; Collegamento dei dati idonei a rivelare lo stato di salute o la vita sessuale con informazioni relative a pagamenti, esenzioni o corretta prescrizione di medicinali; Elaborazione di dati raccolti da terzi; Operazioni di trattamento affidate in parte a	Acquisizione e caricamento dati; Consultazione; Comunicazione a terzi.

	terzi; Organizzazione in banche dati; Raccolta di dati presso l'interessato; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Trattamenti temporanei finalizzati ad una rapida aggregazione di dati o alla loro trasformazione in forma anonima; Trattamento di dati mediante prelievo di materiale biologico; Collegamento dei dati idonei a rivelare lo stato di salute o la vita sessuale con informazioni relative a pagamenti, esenzioni o corretta prescrizione di medicinali; Raccolta di dati a fini di trattamento da parte di terzi; Raccolta di dati mediante impianti di videosorveglianza; Raccolta di dati per via informatica o telematica; Raccolta di dati presso registri, elenchi, atti o documenti pubblici.	
Presidi Ospedalieri	Organizzazione in banche dati in forma prevalentemente automatizzata; Organizzazione in banche dati in forma prevalentemente non automatizzata; Raccolta di dati mediante strumenti elettronici; Indagini per valutare la suscettibilità a patologie genetiche; Cancellazione di dati immediata o nel breve periodo; Rilevazione sistematica di dati senza particolari elaborazioni; Collegamento dei dati idonei a rivelare lo stato di salute o la vita sessuale con informazioni relative a pagamenti, esenzioni o corretta prescrizione di medicinali; Elaborazione di dati raccolti da terzi; Operazioni di trattamento affidate in parte a terzi; Raccolta di dati a fini di trattamento da parte di terzi; Raccolta di dati presso l'interessato; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Trattamenti temporanei finalizzati ad una rapida aggregazione di dati o alla loro trasformazione in forma anonima; Trattamento di dati mediante prelievo di materiale biologico; Prevenzione nelle popolazioni a rischio genetico; Raccolta di dati mediante impianti di videosorveglianza.	Acquisizione e caricamento dati; Consultazione; Comunicazione a terzi.
Dipartimento di Prevenzione	Conservazione dei dati per lungo periodo; Organizzazione in banche dati; Rilevazione sistematica di dati senza particolari elaborazioni; Trattamento informatico; Trattamento cartaceo; Raccolta di dati presso l'interessato; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Raccolta di dati presso terzi; Inserimento in banche dati; Elaborazione ed aggiornamento di dati; Raccolta di dati presso registri e in banca dati; Trattamento in via informatica – ARVET; Elaborazione di dati raccolti da terzi; Operazioni di trattamento affidate in parte a terzi; Raccolta di dati a fini di trattamento da parte di terzi; Raccolta di dati mediante strumenti elettronici; Trattamenti temporanei finalizzati ad una rapida aggregazione di dati o alla loro trasformazione in forma anonima; Trattamento di dati mediante prelievo biologico.	Acquisizione e caricamento dati; Consultazione; Comunicazione a terzi; Conservazione.
Dipartimento di Salute Mentale	Collegamento dei dati idonei a rivelare lo stato di salute o la vita sessuale con informazioni relative a pagamenti, esenzioni o corretta prescrizione di medicinali; Raccolta di dati presso l'interessato; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Definizione della personalità e dei profili dell'interessato; Raccolta di dati tramite schede, questionari e test psicoattitudinali; Associazione di più dati biometrici; Organizzazione degli archivi in banche dati; Raccolta di dati mediante strumenti elettronici; Organizzazione in banche dati in forma prevalentemente non automatizzata; Raccolta di dati per via informatica o telematica; Raccolta di dati c/o registri, elenchi, atti o documenti pubblici.	Tutela della salute mentale
Dipartimento del Farmaco	Collegamento dei dati idonei a rivelare lo stato di salute o la vita sessuale con informazioni relative a pagamenti, esenzioni o corretta prescrizione di medicinali; Elaborazione di dati raccolti da terzi; Operazioni di trattamento affidate in parte a terzi; Organizzazione in banche dati; Raccolta di dati a fini di trattamento da parte di terzi; Raccolta di dati presso l'interessato; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Raccolta di dati presso terzi; Controllo dell'appropriatezza delle prescrizioni farmaceutiche; Gestione pratiche	Acquisizione e caricamento dati; Consultazione; Comunicazione a terzi.

	prestazioni integrative.	
Dipartimento delle Dipendenze	Interventi su tossicodipendenti e alcooldipendenti; Interventi di prevenzione nelle scuole e fabbriche; Formazione con strutture di volontariato.	Registrazione, aggiornamento, consultazione e gestione dei pazienti trattati.
SOC Medicina Legale	Acquisizione ed archiviazione dati, loro gestione; Consultazione e conservazione.	Acquisizione ed archiviazione dati; Consultazione.
Direzione Socio Assistenziale Distretto di Casale	Organizzazione in banche dati; Raccolta di dati mediante strumenti elettronici; Raccolta di dati presso l'interessato; Raccolta di dati presso organismi e strutture del servizio sanitario nazionale; Raccolta di dati presso terzi; Trattamenti temporanei finalizzati ad una rapida aggregazione di dati o alla loro trasformazione in forma anonima.	Acquisizione e caricamento dati; Consultazione; Comunicazione a terzi.
SOC Coordinamento SITRO	Organizzazione in banche dati in forma prevalentemente automatizzata; Organizzazione in banche dati in forma prevalentemente non automatizzata; Raccolta di dati mediante strumenti elettronici; Raccolta di dati presso l'interessato; Raccolta di dati presso terzi.	Acquisizione e caricamento dati; Consultazione.
SOC Servizio Tutela della Salute in Carcere	Rilevamento statistico; Elaborazione dati; Raccolta dati presso l'interessato; Trattamento di dati mediante prelievo di materiale biologico; Raccolta dati presso Strutture del SSN e dell'Amministrazione di Giustizia; Trattamenti temporanei finalizzati ad una rapida aggregazione di dati (flussi informativi previsti dalla legge).	Acquisizione e caricamento dati; Consultazione; Comunicazione a terzi per la tutela della salute in carcere.
Business Unit Libera Professione	Raccolta dati per via informatica o telematica; Raccolta dati presso l'interessato; Raccolta dati presso terzi.	Acquisizione, caricamento, consultazione ed elaborazione dati.

3.3 Distribuzione dei compiti e delle responsabilità

3.3.1. Il Titolare del trattamento

Il Codice istituisce la figura del Titolare, identificandolo nella persona fisica, nella persona giuridica, nella 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.
Il Titolare del trattamento dei dati personali contenuti nelle banche dati dell'Azienda Sanitaria Locale "AL" è la stessa A.S.L. "AL".

3.3.2. Il Responsabile del trattamento

Il Responsabile del Trattamento è la persona fisica preposta dal Titolare al trattamento.
L'ASL AL, con deliberazione n. 1379 del 25.6.2009 e s.m.i., ha individuato quali Responsabili del trattamento dei dati i Responsabili/Referenti di Strutture Operative, ciascuno per le attività svolte e per il trattamento dei dati di rispettiva pertinenza.
La nomina del Responsabile del trattamento è a tempo indeterminato e decade per revoca o per dimissioni dello stesso.
La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso ed eventualmente affidata ad altro soggetto.
Con la suddetta deliberazione sono state adottate linee guida relative ai compiti dei Responsabili del trattamento dei dati (allegato A), trasmesse a ciascun Responsabile unitamente all'atto di nomina.

I responsabili dei trattamenti potranno confrontare le rispettive richieste di abilitazioni e le abilitazioni applicative concesse, secondo le seguenti modalità:

- richiesta scritta del Responsabile
  (anche via email all'indirizzo seg.ced.tortona@aslal.it).

3.3.3. Gli Incaricati del trattamento

Con deliberazione n. 1379 del 25.6.2009 è stato disposto, ai sensi dell'art. 30 del D.Lgs. n. 196/2003, che ogni Responsabile, nell'ambito della struttura di rispettiva competenza, debba provvedere all'individuazione ed alla nomina degli Incaricati che svolgeranno le operazioni di trattamento comunicando agli stessi le istruzioni cui devono attenersi e che vengono allegate al presente Documento sotto la lettera B.

Pertanto, l'ambito di trattamento effettuato sia con che senza strumenti elettronici, consentito ai singoli incaricati, è definito in stretta relazione alla struttura di assegnazione, alla qualifica ricoperta ed ai compiti assegnati dal Dirigente Responsabile e deve intendersi automaticamente modificato in occasione di spostamenti da una struttura all'altra, anche nell'ambito del medesimo Dipartimento ovvero in occasione di mutamenti di mansioni e/o profili funzionali.

Per tutti i trattamenti informatizzati la SC Sistema Informativo inoltrerà in busta chiusa l'elenco delle abilitazioni concesse.

A tale scopo la SC Sistema Informativo dovrà produrre l'elenco aggiornato delle abilitazioni applicative assegnate e vigenti.

In particolare l'Azienda ASL AL ha ritenuto necessario individuare all'interno della SC Sistema Informativo l'Incaricato delle copie di sicurezza dei dati con i seguenti compiti:

- definire e applicare la pianificazione dei salvataggi;
- definire ed applicare le procedure per l'archiviazione dei supporti di memorizzazione;
- definire ed applicare le procedure per la verifica della leggibilità dei supporti di memorizzazione;
- occuparsi dell'eliminazione dei supporti di memorizzazione;
- curare il reimpiego dei supporti di memorizzazioni utilizzati per i trattamenti di dati personali;
- definire ed applicare le misure per la custodia dei supporti di memorizzazione;
- eseguire periodicamente prove di ripristino dei dati.
- Generare le password, provvedendo a controllare che le password siano univoche.
    - Egli predisporrà l'invio in busta chiusa agli incaricati del trattamento. Tali buste, riconoscibili all'esterno dal nome dell'Incaricato, conterranno le password e l'elenco delle autorizzazioni concesse.

3.3.4. Il Responsabile di Sistema

L'Azienda ASL AL ha ritenuto necessario individuare il direttore della SC Sistema Informativo come Responsabile con le funzioni di Amministratore di sistema con i seguenti compiti:

- garantire le tecnologie atte all'adozione delle misure di sicurezza;
- curare e sovrintendere all'adozione ed applicazione delle misure di sicurezza logica e loro aggiornamenti;
- aggiornare il documento DPS nella parte di sua competenza;
- informare il Titolare nella eventualità che si siano rilevati dei rischi o problemi.

3.3.5. Gli Amministratori di Sistema

L'Azienda ASL AL, in ottemperanza a quanto disposto dal Garante per la protezione dei dati personali con provvedimento del 27.11.2008, ha provveduto, con deliberazione n. 1390 del 30.6.2009, alla nomina degli Amministratori di Sistema, incaricando all'uopo sia

gli operatori interni dell'Azienda che i dipendenti di ditte esterne che svolgono le funzioni di amministratori di sistema sulla base di accordi contrattuali con l'A.S.L. AL.
Le mansioni specifiche dei suddetti Amministratori di Sistema sono dettagliatamente elencate nella deliberazione di cui sopra.

4. Analisi dei rischi che incombono sui dati.

(Regola 19 punto 19.3)

Per una corretta individuazione delle misure di sicurezza da adottare, si è resa necessaria una preliminare attività di analisi e valutazione dei rischi, con ciò intendendosi tutte quelle situazioni, eventi o condotte potenzialmente dannosi e che quindi possono determinare rischi di perdita, distruzione o trattamento illecito dei dati personali.

In particolare l'analisi del rischio costituisce una fase fondamentale di ogni percorso di sicurezza informatica. La sicurezza nell'ambito di un trattamento è condizione necessaria al fine di garantire la riservatezza dei dati dell'interessato. Questo piano programmatico in larga misura tratta dell'adozione di misure minime di sicurezza, obbligatorie per legge, e quindi non graduabili. La valutazione del rischio sarà comunque utilizzata per tutte quelle situazioni in cui l'adozione di misure minime sia non sufficiente e pertanto si debba valutare una gradazione delle misure adottabili. La valutazione dei rischi connessi e un piano di adeguamento per ridurli, per cui è necessaria una analisi con lo scopo di monitorare lo stato dei processi aziendali, di classificare i rischi connessi, di segnalarli ai responsabili e di indicare i tempi di adeguamento.

In tali contesti, cioè qualora sia necessaria una graduazione delle misure adottabili, si adotta una valutazione del rischio basata sui seguenti criteri :

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

In particolare:

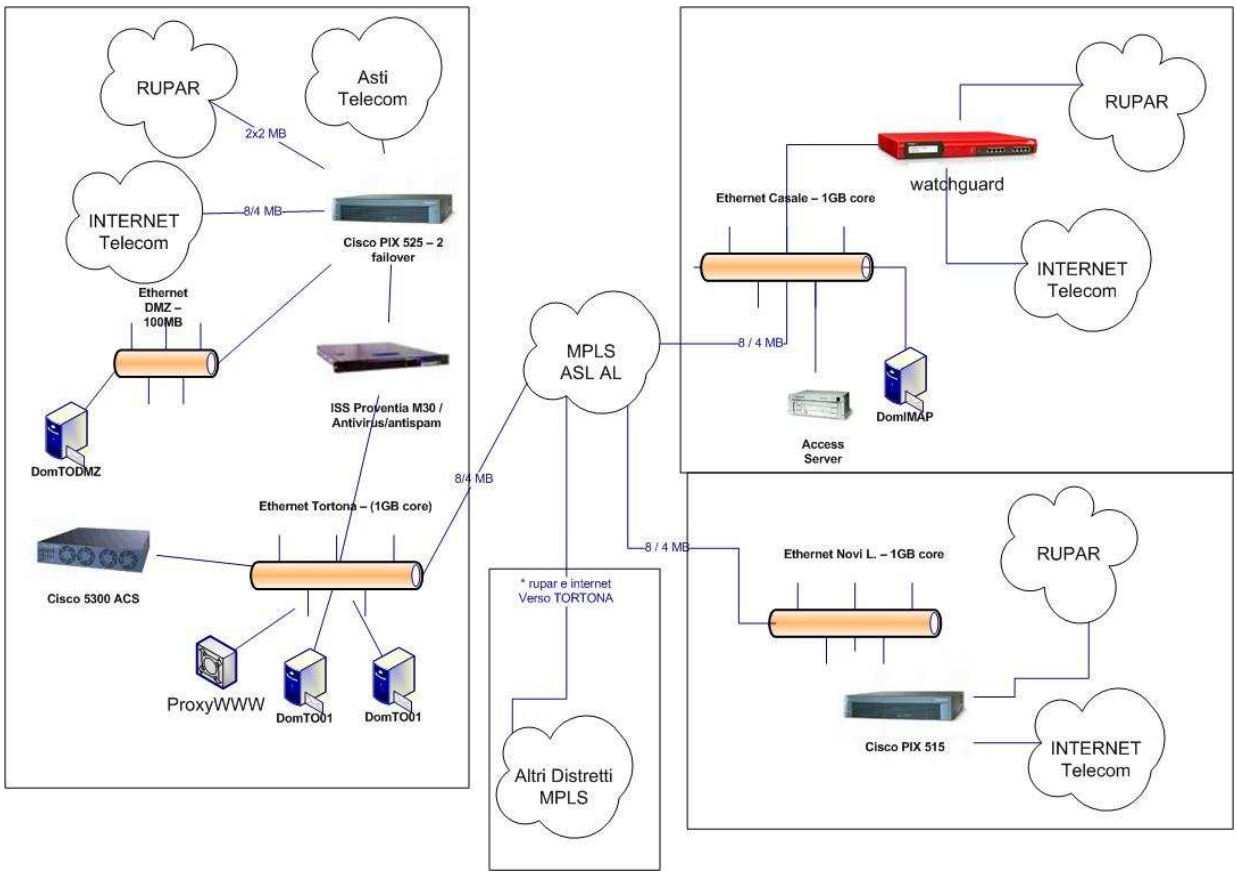
3. si considerano gravi le minacce che possono limitare la disponibilità di servizi informatici a supporto delle attività assistenziali o delle attività rese al pubblico
4. si considerano gravi le minacce che portano alla modifica illecita di messaggi – e quindi di informazioni gestite dall'azienda - qualora tali messaggi abbiano un valore medico-legale o la loro modifica comporti un danno patrimoniale per l'azienda
5. si considerano gravi le minacce di fraudolenta impersonificazione – qualora ciò porti alla produzione di falsi atti con valore medico-legale o che comportino un danno patrimoniale per l'azienda
6. si considerano gravi le minacce di fraudolenta impersonificazione – qualora ciò porti alla modifica fraudolenta di atti con valore medico-legale originariamente legittimi, o qualora ciò porti ad un danno patrimoniale per l'azienda
7. si considerano gravi le minacce di intercettazione qualora i dati intercettabili riguardino dati personali di natura sensibile ai sensi della legge sulla tutela dei dati personali.

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

Da tali analisi e della localizzazione delle postazioni di lavoro e dei servizi si evince che:

- le postazioni di lavoro sono interamente collocate entro il confine aziendale e fruisce di servizi applicativi localizzati entro il confine aziendale.
- Esistono alcune utenze collocate fuori dalla rete aziendale che accedono a funzionalità applicative gestite su server di competenza dell'Azienda tramite connessione su rete privata circuito Consip su protocollo MPLS / TCP adibite all'assistenza tecnica e alle connessioni con medici convenzionati.

L'architettura che offre il miglior rapporto fra minimizzazione dei i rischi complessivi del sistema e costi di realizzazione e gestione è del tipo seguente:



Tale architettura si basa sui seguenti criteri:

- Firewall – gestione anti intrusione per connessione ad internet e a enti esterni. Definisce un confine aziendale definito, con solo tre punti di attraversamento presidiati da dispositivi facilmente controllabili, gestibili e monitorabili, uno per ex ASL;
- RAS Server – Server di autentificazione per le connessione telefoniche e/o remote a utenti al di fuori del normale confine aziendale
- Internet – con la doppia veste di mezzo di comunicazione per gli utenti aziendali che accedono in VPN e insieme di risorse accedute dai client posti nella intranet aziendale
- Intranet – sede della maggior parte dei client aziendale e dei server che erogano la maggior parte delle funzionalità applicative
- DMZ – sede di alcuni sistemi che devono essere visibili in internet, ma svolgono anche servizi applicativi aziendali. Definisce un'area con caratteristiche di sicurezza

intermedia fra zona interna ed esterna in cui porre i sistemi che svolgono servizi applicativi per gli utenti esterni che vengono veicolati da Internet;
- PSTN – mezzo di comunicazione per quegli utenti che non hanno accesso ad internet
- Defender – Gateway Level II in grado di controllare il traffico di rete SMTP / HTTP / POP3 e filtrare i messaggi affetti da virus e i contenuti del traffico internet.

L'attuazione delle misure tecniche che conducono alla realizzazione di una tale infrastruttura sono di competenza del Servizio Informativo Aziendale. Così come la successiva gestione di tale infrastruttura.

Per quanto riguarda le banche dati descritte nei precedenti paragrafi si possono individuare 3 sedi fisico-ambientali diverse con la relativa analisi dei rischi:
- Sede 1: SC Sistema Informativo sede di TORTONA;
  - eventi relativi al contesto fisico ambientale: i locali sono protetti da sistema di allarme, sono dotati di sistema antincendio, impianto di climatizzatore, gruppo di continuità. Può accedere solo personale a seguito di sottoscrizione di apposito modulo per l'utilizzo delle chiavi di accesso;
  - eventi relativi agli strumenti: l'accesso alle banche dati è consentito solo alle persone autorizzate con credenziali di autenticazione di accesso.
- Sede 2: SOC Sistema Informativo sedi di CASALE Monferrato;
  - eventi relativi al contesto fisico ambientale: i locali sono protetti da sistema di allarme, sono dotati di sistema antincendio, impianto di climatizzatore, gruppo di continuità.
  - eventi relativi agli strumenti: l'accesso alle banche dati è consentito solo alle persone autorizzate con credenziali di autenticazione di accesso.
- Sede 3: Servizio Informatica sede di NOVI Ligure;
  - eventi relativi al contesto fisico ambientale: i locali NON sono protetti da sistema di allarme, sono dotati di sistema antincendio. L'accesso ai locali è consentito solo agli operatori incaricati, ma non è controllato.
  - eventi relativi agli strumenti: l'accesso alle banche dati è consentito solo alle persone autorizzate con credenziali di accesso.
- Presidi Ospedalieri e tutte le altre sedi operative

La valutazione dei rischi ha permesso di evidenziare due categorie di trattamenti:
- i trattamenti che interessano banche dati e risorse dei sistemi centrali, in gestione alla SC Sistema Informativo;
- i trattamenti che interessano banche dati su condivisione distribuite, in gestione alle altre Strutture aziendali.

In tali contesti, cioè qualora sia necessaria una graduazione delle misure adottabili, si adotta una valutazione del rischio basata sui seguenti criteri :

Non evidenziabile	Rischio accettabile che non pregiudica in modo rilevante il trattamento dati
Basso	Rischio che richiede un intervento programmabile a lungo termine
Medio	Rischio che richiede un intervento a medio termine
Alto	Rischio che richiede un interevento immediato

Nella tabella che segue sono riportati in via sintetica i risultati dell'attività di cui sopra.

Tab. 3 – Analisi dei rischi

Rischi		Sede 1-2-3	Altre sedi
		Gravità stimata	
Eventi relativi agli operatori	Sottrazione di credenziali di autenticazione	Bassa: le informazioni viaggiano solo su rete privata.	Bassa: le informazioni viaggiano solo su rete privata.
	Carenza di consapevolezza, disattenzione o incuria	Media: in alcuni casi più operatori utilizzano le stesse credenziali.	Media: a causa della noncuranza nella conservazione delle credenziali di autenticazione queste potrebbero essere sottratte al legittimo possessore ed utilizzate in modo improprio; è tuttavia prevista la modifica programmata delle password.
	Comportamenti sleali o fraudolenti	Non ci sono rischi evidenziabili.	Non ci sono rischi evidenziabili.
	Errore materiale	Non evidenziabile: gli strumenti hanno architettura ridondata e le procedure di backup garantiscono il recupero.	Non evidenziabile: per i trattamenti effettuati su area server, considerata la tipologia degli strumenti utilizzati e le regolari procedure di backup, la minaccia non pregiudica in modo rilevante il trattamento dei dati. Alta: per i trattamenti memorizzati su disco locale.
Eventi relativi agli strumenti	Azione di virus informatici o di programmi suscettibili di recare danno	Non evidenziabile: i sistemi sono protetti da software antivirus.	Non evidenziabile: i sistemi sono protetti da software antivirus.
	Spamming o tecniche di sabotaggio	Non evidenziabile: i sistemi sono protetti da software antispam.	Non evidenziabile: i sistemi sono protetti da software antispam.
	Malfunzionamento, indisponibilità o degrado degli strumenti	Bassa: i sistemi sono configurati con livelli architetturali di ridondanza.	Alta: le stazioni individuali non prevedono alcun livello di ridondanza.
	Accessi esterni non autorizzati	Bassa: tutte le linee esterne sono protette da firewall.	Bassa: tutte le linee esterne sono protette da firewall.
	Intercettazione di informazioni in rete	Bassa: non esiste al momento un dispositivo in grado di evidenziare tali attività.	Bassa: non esiste al momento un dispositivo in grado di evidenziare tali attività.
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	Media: i locali sono presidiati con chiusure meccaniche ma non tutti sono dotati di antiintrusione.	Media: pur essendo presidiati in orario di servizio, non tutti i locali sono dotati di chiusura meccanica o di sistemi antiintrusione.
	Sottrazione di strumenti contenenti	Media: i locali sono presidiati con chiusure	Media: Pur essendo presidiati in orario di servizio, non tutti i

	dati	meccaniche ma non tutti sono dotati di antiintrusione.	locali sono dotati di chiusura meccanica o di sistemi antiintrusione.
	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria	Bassa: i locali sono dotati di impianti antincendio e climatizzatore periodicamente controllati; in generale non risultano rischi specifici prevedibili e probabili, correlati alla ubicazione geografica dei centri elaborazione dati.	Media: In generale non risultano rischi specifici prevedibili e probabili, correlati alla ubicazione geografica dei diversi siti della A.S.L. ma non tutti i locali sono dotati di impianti idonei a fronteggiare gli eventi distruttivi.
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Bassa: i locali sono dotati di gruppi di continuità dedicati e impianti di climatizzazione.	Media: non tutte le strutture aziendali sono dotate di impianti idonei.
	Errori umani nella gestione della sicurezza fisica	Bassa: competenza acquisita degli operatori e presenza di copie fisiche di riserva.	Bassa: competenza acquisita degli operatori e presenza di copie fisiche di riserva.

Ai fini della determinazione della frequenza della minaccia si stabiliscono i seguenti criteri:

- interruzioni alla continuità di servizio dovute a guasti
- interruzioni alla continuità di servizio dovute ad attacchi al sistema.

Di seguito si elencano i sistemi SERVER presenti distinguendoli in area infrastrutturale e area applicativa.

Per quanto riguarda le interruzioni dovute a guasti si definisce il seguente criterio per la determinazione della probabilità della interruzione:

Tipo di sistema	**Probabilità di interruzione di servizio**
Sistema di tipo SPFF – Single Point of Failure Free : • **nessuno**	
Sistema che adotta tecniche SPFF – Single Point of Failure Free • **Vedi Tab Server Infrastrutturali** • **Vedi Tab Server Applicativi**	Poco probabile
Sistema che non adotta tecniche SPFF – né altri tipi di tutela • **Nessuno**	

Tab. SERVER Infrastrutturali

modello	**Host name**	**Sw di base**	**Servizi Infrastrutturali**	**DBMS**	**Comune**
ACQUI	ACQUI2	Windows 2000	Oracle 7 x	Oracle 7 x	Acqui
ACQUI	NTLAB_ACQUI	Windows 2000 Server	Oracle metafora	Oracle metafora	Acqui
xSeries 335	ATLANTE	Windows 2000	Domini/Active Directory		Alessandria
IOMEGA NAS	NAS-ALESSANDRIA	Windows 2003	FileServer		Alessandria
vmware/esx02	ARCA	Windows 2000	Domini/Active Directory		Casale

vmware/esx03	ARCHIMEDE	Windows 2000 Prof			Casale
vmware	CALIMERO				Casale
vmware/esx04	CASSANDRA	Windows 2003	ADT + Cartelle Cliniche	Sql Server 2005	Casale
vmware/esx01	CASTORE				Casale
	CED partizione lama 1 BCH	AS400			Casale
	CED2 partizione lama1 BCH	AS400			Casale
vmware/esx01	CRUMIRO	Windows 2003	Posta		Casale
vmware	DINOE	Windows 2000	Domini/Active Directory		Casale
	ERIK	Windows 2003	Cartelle Cliniche	Sql Server 2000	Casale
HS21 XM	esx01.asl21.sys lama 2 BCH	ESX 3.5.0 Standard Edition			Casale
HS21 XM	esx02.asl21.sys lama 3 BCH	ESX 3.5.0 Standard Edition			Casale
HS21 XM	esx03.asl21.sys lama 4 BCH	ESX 3.5.0 Standard Edition			Casale
HS21 XM	esx04.asl21.sys lama 5 BCH	ESX 3.5.0 Standard Edition			Casale
vmware/esx04	EUROPA	Windows 2003			Casale
vmware	FERMAT				Casale
HS21	GUTEMBERG lama 6 BCH	Windows 2003 R2	Virtual Center/TSM backup (collegata via SAN a TS3200)		Casale
vmware/esx01	HARPO	Windows 2000	SitoWeb	Sql Server 2000	Casale
	ISIDE				Casale
	LAB partizione lama 1 BCH	AS400			Casale
JS22	lama 1 BCH	AS400, 3 partizioni (CED,CED2,LAB)			Casale
vmware/esx03	MERCURIO	Windows 2000	Posta		Casale
vmware/esx01	NEMESIS				Casale
vmware	NTCED04				Casale
	ORWELL				Casale
vmware/esx03	OSIRIDE				Casale
vmware/esx03	PACMAN				Casale
vmware/esx04	POLLUCE				Casale
Netfinity 5000	PONG		SQL + File Server		Casale
TS3200			Libreria collegata a Lama 6 Blade (Gutemberg)		Casale
TS2230			Tape collegato a lama 1 Blade AS400		Casale
DS4800			SAN per il BCH		Casale
DS4800-exp810			SAN per il BCH		Casale
DS4800-exp810			SAN per il BCH		Casale
DS4800-exp810			SAN per il BCH		Casale
DS4300					Casale
X205	SEDNA				Casale c/o Valenza
PC	CASTSCR	Windows 2000	Domini/Active Directory		Castelnuovo
Novi	NTLAB_NOVI	Windoes2000		Oracle 8	Novi
Novi	NTSCREENING	Windoes2000	Terminal SERVER	SQL Server 2000	Novi
NOVI	NTTBIC22	Windows 2003 Server r2		ACCESS	Novi
NOVI	ntwts22	Windows NT 4.0 Terminal Server			Novi
Novi	PRESENZE22	FEDORA	Proxy	DansGuardian	Novi

NOVI	saneth01/02				Novi
Novi	SERVIZI	FEDORA	Proxy	DansGuardian	Novi
Novi	W2K3BACKUP	Windows 2003	Server Web	LEGATO NETWORKER	Novi
Novi	W2K3DOM1	Windows 2003	Domini/Active Directory		Novi
Novi	W2K3DOM2	Windows 2003	Domini/Active Directory		Novi
Novi	W2K3PROTODB	Windows 2003	Oracle/SQL Protocollo	ORACLE/MSsql	Novi
Novi	W2K3PROWEB	Windows 2003	Server Web	Infoclin	Novi
Novi	W2K3RADIONOVI	Windows 2003	DB Server	SQL Server 2003	Novi
NOVI	w2kl3medleg	Windows 2003 Server r2		ACCESS	Novi
OVADA	NTLAB_OVADA	Windows 2003 Server r2	Oracle metafora	Oracle metafora	Ovada
440	ADE	Windows 2003	Backup		Tortona
vmware ASGARD	ALDEBARAN	Windows 2000	FileServer		Tortona
xSeries 445	ARGO	VmWare ESX 2.1	VMWARE		Tortona
HS21 XM	ASGARD	VmWare ESX3.5	VMWARE		Tortona
xSeries 235	AURIGA	Windows 2000	Domini/Active Directory		Tortona
vmware OLIMPO	CERBERO	Windows 2003	Domini/Active Directory		Tortona
vmware ASGARD	EUROPA	Windows 2000	Domini/Active Directory		Tortona
HS21 XM	GANDALF	RedHat	Posta		Tortona
vmware OLIMPO	LEGOLAS	Windows 2003	Posta		Tortona
vmware OLIMPO	NAS-TORTONA	Windows 2003	FileServer		Tortona
HS21 XM	OLIMPO	VmWare ESX3.5	VMWARE		Tortona
5600	PLUTONE	Windows 2000	Domini/Active Directory		Tortona
vmware OLIMPO	PROXYWWW	Windows 2000	Proxy		Tortona
eSeries 525	SANITARIO	OS400	UGS		Tortona
5500	SATURNO	Windows 2000	Domini/Active Directory		Tortona
HS21 XM	SAURON	RedHat	Posta		Tortona
3000	VENERE	Windows 2000	FileServer		Tortona
xSeries 232	WWW	Windows 2000	Server WEB		Tortona
HS21 XM	ALPHA	Windows 2003	SQL 2005 Cluster		Tortona
HS21 XM	CENTAURI	Windows 2003	SQL 2005 Cluster		Tortona

Tab. SERVER Applicativi

modello	Host name	Sw di base	Particolarità configurazione	Prodotto	Comune
HS21	MERCURIO	Windows 2000	Citrix	Citrix + Euofosoft Medoffice + Eurosoft Infoclin + Metafora Concerto	Tortona
HP Proliant	ATHENA	Windows 2003	Websphere	AccaErre	Tortona
HP Proliant 380	PROMETEO	Windows 2003	HL7 Connect	Metafora TEMPO + Rhapsody	Tortona
HS21	PAGHE	Windows 2003		AccaErre	Tortona
HS21	TRANTOR	Windows 2003	WebServer	Eurosoft CDW + Hospitalweb	Tortona
HS21	NETTUNO1	Windows 2003		x Eurosoft	Tortona
vmware ARCADIA	TRITONE	Windows 2003	HL7 Connect	x Metafora	Tortona
vmware	CARONTE	Windows 2000	FileServer		Tortona

ARCADIA					
vmware ARGO	ENDOR	Windows 2000	Citrix	Citrix + Euofosoft Medoffice + Eurosoft Infoclin + Metafora Concerto	Tortona
vmware OLIMPO	ODINO	Windows 2000	Citrix	Citrix + Euofosoft Medoffice + Eurosoft Infoclin	Tortona
xSeries 232	ARES	Windows 2000	Citrix	Citrix + Euofosoft Medoffice + Eurosoft Infoclin	Tortona
xSeries 445	GIOVE	Windows 2003		IG Consulting DSS Musa	Tortona
vmware ARGO	ANTARES	Windows 2000	Telecup	IBM Websphere	Tortona
	W2keprotodb	Windows 2003		Oracle Metafora	Novi
	w2k3radionovi	Windows 2003		Infoclin	Novi
	w2k3protoweb	Windows 2003		infoclin	Novi
	presenze22	Windows 2000		riweb	Novi
	NTLAB_OVADA	Windows 2003		CONCERTO	Ovada
	NTLAB_ACQUI	WINDOWS 2000	Terminal Server	CONCERTO	Acqui
	nttbic22	WINDOWS 2000	Terminal Server	RUBRICA/ADDEBITI	Ovada
	w2k3medleg	Windows 2003		LIM	Novi
vmware/esx02	ASTERIX	Windows 2003	DSS		Casale
vmware/esx04	CASSANDRA	Windows 2003	ADT + Cartelle Cliniche	Sql Server 2005	Casale
	ERIK	Windows 2003	Cartelle Cliniche	Sql Server 2000	Casale
vmware/esx02	GROUCHO	Windows 2000		Sql Server 2000	Casale

Per quanto riguarda le interruzioni dovute ad attacchi al sistema si definisce il seguente criterio per la determinazione della probabilità della interruzione:

Tipo di sistema	**Probabilità di interruzione di servizio**
Sistemi posti all'interno del confine aziendale • **Vedi Tab Server Infrastrutturali** • **Vedi Tab Server Applicativi**	Poco probabile
Sistemi posti al di fuori del confine aziendale o sul confine aziendale, o nella zona demilitarizzata, o accessibili da utenti posti al di fuori del confine aziendale • **Vedi Tab. DMZ**	Mediamente probabile

Tab. DMZ

modello	**Host name**	**Sw di base**	**Servizi Infrastrutturali**	**Comune**
HP Proliant	EPIDEM1	RedHat	Server WEB	Tortona
HP Proliant	EPIDEM2	RedHat	Server WEB	Tortona
HS21	ARAGORN	Windows 2003	Lotus Domino	Tortona

- **Minacce di modifica illecita**

Per quanto riguarda la modifica illecita si definisce il seguente criterio per la determinazione della probabilità di accadimento:

Tipo di sistema	Probabilità di modifica illecita
Sistemi posti all'interno del confine aziendale • **Vedi Tab Server Infrastrutturali** • **Vedi Tab Server Applicativi**	Poco probabile
Sistemi posti al di fuori del confine aziendale o sul confine aziendale, o nella zona demilitarizzata, o accessibili da utenti posti al di fuori del confine aziendale • **Nessuno**	Altamente probabile

Per quanto riguarda la fraudolenta impersonificazione si definisce il seguente criterio per la determinazione della probabilità di accadimento:

Tipo di sistema	Probabilità di fraudolenta impersonificazione
Sistemi posti all'interno del confine aziendale • **Vedi Tab Server Infrastrutturali** • **Vedi Tab Server Applicativi**	Poco probabile
Sistemi posti al di fuori del confine aziendale o sul confine aziendale, o nella zona demilitarizzata, o accessibili da utenti posti al di fuori del confine aziendale • **Nessuno**	Altamente probabile

5. Misure in essere e da adottare.

(Regola 19 punto 19.4)

Gli obiettivi di sicurezza che l'A.S.L. AL si pone con la redazione del seguente piano e con l'adozione delle misure di sicurezza previsti sono:

- dare attuazione sia a quanto previsto nel D.Lgs. 196/2003 sia a misure di sicurezza ulteriori che l'Azienda ritenga opportune e necessarie nell'ottica del perseguimento degli obiettivi istituzionalmente attribuiti;
- Ridurre a livelli accettabili i principali rischi di sicurezza a cui il sistema per il trattamento dei dati è sottoposto;
- Mantenere, compatibilmente con i vincoli di sicurezza enunciati, il massimo livello di utilizzabilità del sistema.

Si ritiene che gli obiettivi di sicurezza siano raggiungibili tramite la predisposizione delle seguenti misure:

- attuazione delle misure di tutela fisica degli apparati;
- attuazione della sicurezza logica degli apparati;
- attuazione delle misure di sicurezza per la protezione delle aree e dei locali ove si svolge il trattamento dei dati personali;
- attuazione delle misure di sicurezza per la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;

- attuazione delle misure organizzative e tecniche per la gestione dei documenti informatici.

L'ASL AL adotta un Regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003 (allegato C).
Nella seguente tabella sono riportate le misure di sicurezza che, tenendo conto della natura del rischio, sono poste come norme di carattere generale di tutela degli ambienti in cui avviene il trattamento dei dati, di tutela delle apparecchiature e delle procedure informatiche e dei supporti cartacei, fotografici e magnetico-elettronici.

Tab. 4 – Misure di sicurezza adottate o da adottare

LOCALI CED

C01	***Comportamenti degli operatori***
Evento che si intende contrastare	Sottrazione di credenziali di autenticazione
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	Sono stati adottati profili di autorizzazioni specifici per ogni operatore, cui verrà richiesta la modifica della password di ingresso in modo periodico. Sono state inoltre create credenziali specifiche per la configurazione di quei servizi / processi che necessitano di specifici profili utente.
Misure da adottare	E' necessario completare alcune procedure relativamente ai servizi di alcuni server e separare questi dai profili di amministrazione utilizzati normalmente per accedere fisicamente alle console dei server.

C02	***Comportamenti degli operatori***
Evento che si intende contrastare	Carenza di consapevolezza, disattenzione o incuria. Comportamenti sleali o fraudolenti.
Trattamenti interessati	Tutti i trattamenti
Misure adottate	E' stata avviata un'attività di formazione del personale per renderlo edotto nel trattamento dei rischi individuati e dei modi per prevenire i danni al sistema di elaborazione e gestione logica dei dati. L'utilizzo delle procedure informatizzate o elettroniche che trattano dati personali o sensibili è consentito al personale autorizzato dal responsabile del servizio di afferenza. L'ASL AL adotta un Regolamento sulle misure di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite Istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Occorre consolidare le procedure organizzative di concessione delle autorizzazioni al fine di uniformare i comportamenti in tutto il territorio dell'ASL.

C03	***Comportamenti degli operatori***
Evento che si intende contrastare	Errori materiali
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	Tutti i sistemi informatizzati sono gestiti da sistemi di backup che consentono il recupero delle informazioni potenzialmente danneggiate. I dati sono recuperabili all'ultimo backup effettuato tranne per i server SQL per cui esiste un salvataggio incrementale a mezza giornata.
Misure da adottare	Occorre completare il consolidamento della gestione centralizzata dei salvataggi presso la sede di Novi Ligure.

C04	***Eventi relativi agli strumenti***
Evento che si intende contrastare	Azione di virus informatici o di programmi suscettibili di recare danno
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	Tutti i PC e i Server sono in rete e integrati nel dominio aziandale. Su tutti i PC e Server è installata una protezione antivirus aggiornata quotidianamente.

Misure da adottare	Completamento configurazione e messa in dominio

C05	***Eventi relativi agli strumenti***
Evento che si intende contrastare	Spamming o tecniche di sabotaggio
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	E' attivata la protezione anti-spam di Panda Antivirus e IBM ISS a livello centralizzato
Misure da adottare	nessuna

C07	***Eventi relativi agli strumenti***
Evento che si intende contrastare	Accessi esterni non autorizzati
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	Tutti i collegamenti esterni sono protetti da firewall, impedendo quindi ogni traffico entrante verso la rete aziendale
Misure da adottare	Occorre uniformare le attuali configurazioni delle tre diverse sedi.

C08	***Eventi relativi agli strumenti***
Evento che si intende contrastare	Intercettazione di informazioni in rete
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	Nessuna misura è stata al momento adottata
Misure da adottare	/

C09	***Eventi relativi al contesto***
Evento che si intende contrastare	Accessi non autorizzati a locali/reparti ad accesso ristretto
Trattamenti interessati	Tutti i trattamenti.
Misure adottate	I locali sono costantemente presidiati da personale durante il giorno. Allo scadere dell'orario di lavoro i locali vengono chiuse e nessun utente dei servizi è ammesso, se non personalmente accompagnato da personale autorizzato. L'ASL AL adotta un Regolamento sulle misure di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite Istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati. Solo la sede di Tortona è protetta da un sistema di allarme anti intrusione con porte blindate.
Misure da adottare	Estendere l'adozione delle misure antiintrusione nei locali.

C10	***Eventi relativi al contesto***
Evento che si intende contrastare	Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria.
Trattamenti interessati	Tutti i trattamenti
Misure adottate	I locali di tutte le sedi sono dotati di estintori per la soppressione di focolai di incendio disposti secondo le normative vigenti e piano antincendio, tranne la sede di Casale. L'ASL AL adotta un Regolamento sulle misure di sicurezza in attuazione del D.Lgs. 196/2003.
Misure da adottare	Tutti i locali dovranno essere dotati di idonei impianti antincendio.

C11	***Eventi relativi al contesto***
Evento che si intende	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)

contrastare	
Trattamenti interessati	Trattamenti di tipo informatico.
Misure adottate	I server in gestione al personale del Servizio informatica sono tutti collegati ad un gruppo di continuità. Tale gruppo garantisce stabilità alla tensione in ingresso e assicura un'autonomia temporale necessaria ad avviare le corrette procedure di spegnimento dell'elaboratore. I locali del Servizio Informatica sono dotati di impianto di climatizzazione. La maggior parte dei locali è dotata di impianti di climatizzazione.
Misure da adottare	Tutti gli altri locali dove vengono eseguiti trattamenti di tipo informatico dovranno possedere condizioni idonee di microclima, in termini di temperatura, polverosità, umidità e, nel caso questo non sia garantibile attraverso misure passive, andranno predisposte le adeguate misure attive di condizionamento.

C12	***Eventi relativi al contesto***
Evento che si intende contrastare	Errori umani nella gestione della sicurezza fisica
Trattamenti interessati	Tutti i trattamenti
Misure adottate	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti, sono effettuati periodicamente. Sono previsti procedimenti di salvataggio dei dati. Vengono effettuate copie fisiche di riserva presso opportune casseforti ignifughe.
Misure da adottare	Si prevede la redazione di un opuscolo informativo diretto al personale neo assunto avente ad oggetto il "Codice Privacy".

ALTRI LOCALI

L01	***Comportamenti degli operatori***
Evento che si intende contrastare	Sottrazione di credenziali di autenticazione
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	• Il trattamento di dati personali è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti • Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dall' interessato. • Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione • Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Pertanto si dispone che ogni utente definito, non venga più cancellato, ma disabilitato nel caso cessi di essere in uso, in maniera tale da evitarne il riutilizzo (D.L. 196/2003 Allegato B) • La parola chiave, prevista dai sistemi di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti al proprio nome utente o ai propri dati anagrafici, deve contenere almeno tre dei seguenti quattro gruppi di caratteri : lettere maiuscole dalla A alla Z, lettere minuscole dalla a alla z, numeri (0 – 9) e caratteri speciali come !, $, #, %. La password dovrà essere modificata al primo utilizzo e, successivamente, almeno ogni 90 giorni. In qualsiasi momento ogni incaricato potrà modificare la propria password mediante l'ausilio della procedura informatizzata perché diversa dalle tre precedenti (D.Lgs. 196/2003 Allegato B, punti 5) Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione tre Aziende avevano provveduto ad adottare. L'ASL AL adotta un Regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Proseguire l'istruzione degli incaricati sulle corrette modalità di gestione autonoma delle credenziali. Proseguire l'istruzione degli incaricati sulla corretta gestione degli strumenti elettronici. Migliorare la gestione dei profili di autorizzazione, con particolare riferimento alla gestione

	degli stessi da parte delle applicazioni informatiche più datate. Implementazione delle misure di sicurezza.

L02	***Comportamenti degli operatori***
Evento che si intende contrastare	Carenza di consapevolezza, disattenzione o incuria. Comportamenti sleali o fraudolenti.
Trattamenti interessati	Tutti i trattamenti
Misure adottate	E' già stata avviata un'attività di formazione del personale per renderlo edotto nel trattamento dei rischi individuati e dei modi per prevenire i danni al sistema di elaborazione e gestione logica dei dati. L'utilizzo delle procedure informatizzate o elettroniche che trattano dati personali o sensibili è consentito al personale autorizzato dal responsabile del servizio di afferenza. L'ASL AL adotta un Regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Sono previsti ulteriori incontri formativi di sensibilizzazione, informazione e aggiornamento agli incaricati e Responsabili sulla corretta modalità operativa per il trattamento dei dati e sui nuovi strumenti e/o misure di sicurezza implementati dall'Azienda. Implementazione delle misure di sicurezza.

L03	***Comportamenti degli operatori***
Evento che si intende contrastare	Errori materiali
Trattamenti interessati	Tutti i trattamenti
Misure adottate	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti, sono effettuati periodicamente. Quando emerge un problema di sicurezza viene attivato un team di risposta per gli incidenti da guasto guidato dal Responsabile della sicurezza dei dati e dei sistemi. Qualora il sistema risulti compromesso, totalmente o in parte, verranno adottate le disposizioni contenute nel Capitolo 6 del presente DPS. Sono previsti procedimenti di salvataggio dei dati. L'ASL AL adotta un Regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Implementazione delle misure di sicurezza.

L04	***Eventi relativi agli strumenti***
Evento che si intende contrastare	Azione di virus informatici o di programmi suscettibili di recare danno
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	Su ogni stazione collegata alla rete aziendale è installato software antivirus in grado di scaricare nuove firme virali almeno una volta al giorno.
Misure da adottare	Verifica periodica dell'aggiornamento delle stazioni.

L05	***Eventi relativi agli strumenti***
Evento che si intende contrastare	Malfunzionamento, indisponibilità o degrado degli strumenti
Trattamenti interessati	Trattamenti di tipo informatico
Misure adottate	Esiste un regolamento aziendale sulla manutenzione dei p.c. che garantisce la riparazione da guasti e malfunzionamenti tramite una ditta esterna specializzata. E' in atto un'analisi della vetustà degli strumenti in uso al fine di aggiornare l'intero parco macchine.
Misure da adottare	E' prevista l'estensione della manutenzione su tutti i p.c. aziendali. E' prevista la sostituzione di tutti i macchinari obsoleti.

L06	***Eventi relativi al contesto***

Evento che si intende contrastare	Accessi non autorizzati a locali/reparti ad accesso ristretto
Trattamenti interessati	Tutti i trattamenti.
Misure adottate	Alcune sedi sono protette da un sistema di allarme antiintrusione. I locali sono costantemente presidiati da personale durante il giorno. Allo scadere dell'orario di sportello, le porte di accesso vengono chiuse e nessun utente dei servizi è ammesso, se non personalmente accompagnato da personale autorizzato. Il personale dipendente timbra ogni giorno l'entrata/uscita per l'accesso agli uffici; per gli utenti ed i visitatori non esiste una registrazione ad eccezione degli uffici che erogano servizi al pubblico e del Pronto Soccorso, le cui modalità sono diversificate in funzione dei servizi erogati agli utenti che usufruiscono delle prestazioni. I flussi relativi a personale non dipendente sono identificabili in due tipologie: gli assistiti ed eventuali parenti o affini ed i terzi prestatori d'opera. In entrambi i casi il personale consente loro l'accesso ai locali filtrandoli al momento del loro ingresso. Gli addetti sono tenuti ad effettuare vigilanza contro il rischio di accesso di persone non autorizzate. L'ASL AL adotta un regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite Istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Estendere l'adozione delle misure antiintrusione nei locali. Implementazione delle misure di sicurezza.

L07	***Eventi relativi al contesto***
Evento che si intende contrastare	Sottrazione di strumenti contenenti dati
Trattamenti interessati	Tutti i trattamenti
Misure adottate	Alcune sedi sono protette da un sistema di allarme antiintrusione. I locali sono costantemente presidiati da personale durante il giorno. Allo scadere dell'orario di sportello, le porte di accesso vengono chiuse e nessun utente dei servizi è ammesso, se non personalmente accompagnato da personale autorizzato. Il personale dipendente timbra ogni giorno l'entrata/uscita per l'accesso agli uffici; per gli utenti ed i visitatori non esiste una registrazione ad eccezione degli uffici che erogano servizi al pubblico e del Pronto Soccorso, le cui modalità sono diversificate in funzione dei servizi erogati agli utenti che usufruiscono delle prestazioni. I flussi relativi a personale non dipendente sono identificabili in due tipologie: gli assistiti ed eventuali parenti o affini ed i terzi prestatori d'opera. In entrambi i casi il personale consente loro l'accesso ai locali filtrandoli al momento del loro ingresso. Gli addetti sono tenuti ad effettuare vigilanza contro il rischio di accesso di persone non autorizzate. L'ASL AL adotta un regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite Istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Estendere l'adozione delle misure antiintrusione nei locali. Sono previste misure per la gestione dei dati sensibili esclusivamente su area server. Implementazione delle misure di sicurezza.

L08	***Eventi relativi al contesto***
Evento che si intende contrastare	Eventi distruttivi, naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria.
Trattamenti interessati	Tutti i trattamenti
Misure adottate	I locali di tutte le sedi sono dotati di estintori per la soppressione di focolai di incendio disposti secondo le normative vigenti e piano antincendio. Alcuni locali sono dotati di un adeguato impianto antincendio. L'ASL AL adotta un regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite Istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Tutti i locali dovranno essere dotati di idonei impianti antincendio. Implementazione delle misure di sicurezza.

L09	***Eventi relativi al contesto***
Evento che si intende contrastare	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)
Trattamenti	Trattamenti di tipo informatico.

interessati	
Misure adottate	La maggior parte dei locali che gestiscono stazioni di front office è ubicata all'interno del perimetro ospedaliero e quindi dotata di UPS. La maggior parte dei locali è dotata di impianti di climatizzazione.
Misure da adottare	Tutti gli altri locali dove vengono eseguiti trattamenti di tipo informatico dovranno possedere condizioni idonee di microclima, in termini di temperatura, polverosità, umidità e, nel caso questo non sia garantibile attraverso misure passive, andranno predisposte le adeguate misure attive di condizionamento.

L10	***Eventi relativi al contesto***
Evento che si intende contrastare	Errori umani nella gestione della sicurezza fisica
Trattamenti interessati	Tutti i trattamenti
Misure adottate	Gli aggiornamenti periodici dei programmi, volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne i difetti, sono effettuati periodicamente . Quando emerge un problema di sicurezza viene attivato un team di risposta per gli incidenti da guasto guidato dal Responsabile della sicurezza dei dati e dei sistemi. Qualora il sistema risulti compromesso, totalmente o in parte, verranno adottate le disposizioni contenute nel piano di continuità ed emergenza. Sono previsti procedimenti di salvataggio dei dati. Vengono effettuate copie fisiche di riserva. Sono stati effettuati incontri formativi per istruire e sensibilizzare il personale relativamente al trattamento dei dati personali, in particolare per quanto concerne i dati sensibili sanitari. L'ASL AL adotta un regolamento sulle misure minime di sicurezza in attuazione del D.Lgs. 196/2003. L'ASL AL adotta apposite Istruzioni sui compiti dei Responsabili e sulle attività degli Incaricati del trattamento dei dati.
Misure da adottare	Si prevede la redazione di un opuscolo informativo diretto al personale neo assunto avente ad oggetto il "Codice Privacy". Implementazione delle misure di sicurezza.

Tutti gli apparati attivi di rete andranno collocati in armadi chiusi a chiave che garantiscano le seguenti caratteristiche di microclima:

- valori corretti di temperatura
- valori corretti di polverosità
- valori corretti di umidità.

Per quegli armadi che risultino essere particolarmente sollecitati dalle prove di carico del gruppo elettrogeno andranno previsti opportuni stabilizzatori in grado di limitare le sovratensioni generate dalla partenza del gruppo elettrogeno.

Sono inoltre adottate le seguenti misure minime di sicurezza relative a trattamenti che vengono messi a disposizione come servizi di elaboratori connessi in rete:

1. Il trattamento di dati personali è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dall' interessato.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione
4. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Pertanto si dispone che ogni utente definito, non venga più cancellato, ma disabilitato nel caso cessi di essere in uso, in maniera tale da evitarne il riutilizzo (D.L. 196/2003 Allegato B)

5. La parola chiave, prevista dai sistemi di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti al proprio nome utente o ai propri dati anagrafici, deve contenere almeno tre dei seguenti quattro gruppi di caratteri : lettere maiuscole dalla A alla Z, lettere minuscole dalla a alla z, numeri (0 – 9) e caratteri speciali come !, $, #, %. La password dovrà essere modificata al primo utilizzo e, successivamente, almeno ogni 90 giorni. In qualsiasi momento ogni incaricato potrà modificare la propria password mediante l'ausilio della procedura informatizzata perché diversa dalle tre precedenti (D.L. 196/2003 Allegato B, punto 5)
6. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento
7. Il reimpiego dei supporti di memorizzazione è vietato qualora siano serviti per la memorizzazione di dati sensibili.

È responsabile della formulazione di opportune politiche di gestione dei sistemi di elaborazione che garantiscano il rispetto delle misure minime di sicurezza – e della predisposizione delle misure attuative, per la parte di competenza – il Servizio Informativo Aziendale.

6. Criteri e modalità di ripristino della disponibilità dei dati
(Regola 19 punto 19.5)

Al fine di tutelare adeguatamente i dati gestiti nei vari sistemi di elaborazione è necessario predisporre un adeguato piano di backup.
A tal fine si dispone quanto segue:

- I salvataggi sono programmati in modo automatizzato quotidianamente durante il periodo I salvataggi sono programmati in modo automatizzato quotidianamente durante il periodo notturno.
- Il salvataggio è effettuato in modo incrementale mantenendo le ultime 21 modifiche, per un periodo massimo di 31 giorni. Verrà conservata per ulteriori 60 giorni l'ultima copia ancora memorizzata nel sistema.
- la programmazione dei salvataggi è conservata per iscritto nella scheda dei backup dei server.
- I supporti fisici contenenti i backup andranno conservati in luogo sicuro e diverso da quello dove ha sede il server corrispondente, in maniera tale da minimizzare la probabilità di distruzione contestuale di server e dati di salvataggio. Tali supporti andranno conservati in armadi ignifughi chiusi a chiave, o comunque in luoghi che abbiano un ragionevole grado di resistenza agli incendi

È responsabile della formulazione di adeguate politiche di backup il Servizio Informativo Aziendale

6.1 Politiche di gestione dei guasti

Per tutti i trattamenti che occorre tutelare da **minacce alla disponibilità** si adottano le seguenti misure.

Trattamenti per i quali il guasto bloccante è <u>mediamente probabile</u>:

- **Server**

    - **backup quotidiano**
    - **profondità backup di almeno 7 giorni prima dell'evento disastroso**
    - **backup globale mensile**
    - **Conservazione backup in cassaforte ignifuga in locale diverso da quello di dislocazione dei server**
- **Rete**
    - **Adozione di situazioni multi-homed**

Trattamenti per i quali il guasto bloccante è <u>poco probabile:</u>

- **Server**
    - **backup quotidiano**
    - **profondità backup di almeno 7 giorni prima dell'evento disastroso**
    - **Conservazione backup in cassaforte ignifuga in locale diverso da quello di dislocazione dei server**
- **Rete**
    - **Adozione di situazioni multi-homed**

È responsabile della formulazione di adeguate politiche di gestione dei guasti il Servizio Informativo Aziendale.

6.2 Procedure di continuità ed emergenza

Il guasto nell'ambito di un complesso sistema tecnologico, quale il sistema informatico aziendale, è un evento non deterministicamente prevedibile, ma probabilisticamente certo indipendentemente dal grado di sofisticazione degli accorgimenti tecnici messi in atto per aumentare l'affidabilità dei sistemi e il loro grado di ridondanza, pertanto occorre che i responsabili dei trattamenti, di concerto con i servizi tecnici di competenza, predispongano piani opportuni di gestione delle situazioni di malfunzionamento dei sistemi informatici al fine di evitare o minimizzare il disservizio arrecato degli utenti.

Il Piano di continuità operativa dei sistemi per l'elaborazione dell'informazione e del sistema di comunicazione (dati e fonia) generale di azienda viene riportato in appendice. Pertanto si rimanda a quelle indicazioni per tutti quei casi in cui il malfunzionamento della infrastruttura tecnologica porti ad un disservizio nella erogazione della attività aziendale.

La predisposizione e la successiva manutenzione dei Piani di Continuità ed Emergenza è di competenza dei responsabili dei trattamenti – che si possono avvalere, per gli aspetti strettamente tecnici, della collaborazione del Servizio Informativo Aziendale. Qualora non siano stati esplicitamente nominati i responsabili dei trattamenti sarà responsabile di tali aspetti il titolare.

6.3 Procedure di recupero da disastro

Vengono di seguito elencati i trattamenti di cui viene garantito il recupero al giorno successivo l'evento disastroso:

Trattamento	***Banca Dati***	***Ubicazione***
Assistenza Sanitaria;	UGSD00 SANITARIO UGSD00 CED	SC Sistema Informativo Tortona SOC Sistema Informativo Casale

	LHA	
Schede cliniche informatizzate	MedOffice GA	SC Sistema Informativo Tortona SOC Sistema Informativo Casale
Diagnosi dei pazienti strumenti radiologici	SYNAPSE	SC Sistema Informativo Tortona SOC Sistema Informativo Casale SC Informatica Novi
Prenotazione e refertazione di esami clinici o visite specialistiche per via telematica o telefonica	TELECUP	SC Sistema Informativo Tortona SOC Sistema Informativo Casale
Diagnosi dei pazienti strumenti Laboratorio Analisi	METAFORA GELAB	SC Sistema Informativo Tortona SOC Sistema Informativo Casale SC Informatica Novi
Accertamento stato invalidità civile, cecità, sordomutismo, handicap; Per relazioni su cause relative a decessi richieste dall'autorità giudiziaria; Esenzioni ticket per patologia; Assistenza sanitaria; Legge 210/1992.	UGSD00 SANITARIO UGSD00 CED	SC Sistema Informativo Tortona SOC Sistema Informativo Casale

La predisposizione e la successiva manutenzione delle procedure di recupero da disastro è di competenza dei responsabili dei trattamenti e del Servizio Informativo Aziendale che si occuperà degli aspetti strettamente tecnici del recupero dall'evento disastroso.

7. Pianificazione degli interventi formativi

(Regola 19 punto 19.6)

L'Azienda Sanitaria Locale AL ha già avviato un'attività di formazione del personale con l'obiettivo di far conoscere:

- i principi cardine del D.Lgs. 30 giugno 2003, n. 196,
- gli obblighi principali,
- le responsabilità e le sanzioni,
- le regole comportamentali da osservare per trattare in modo sicuro i dati personali,
- i rischi che incombono sui dati e modi per prevenire i danni.

Più precisamente, sono stati tenuti nel corso degli anni incontri formativi che hanno coinvolto tutti i Responsabili dei Dipartimenti, dei Distretti, degli Uffici Amministrativi e di Staff e delle Unità Operative e tutti gli incaricati facenti parte delle varie Strutture aziendali.
Coerentemente con l'evoluzione degli strumenti tecnici adottati dall'Azienda Sanitaria Locale AL, rilevanti rispetto al trattamento di dati personali, e/o all'insorgere di nuove disposizioni legislative in materia verranno istituiti nuovi incontri formativi.
E' stato predisposto un apposito opuscolo informativo avente ad oggetto il "Codice Privacy".

8. Trattamenti affidati all'esterno

(Regola 19 punto 19.7)

Alcuni trattamenti di competenza dell'A.S.L. AL sono stati affidati all'esterno ai soggetti che sono indicati nella tabella 5 seguente.

Il Regolamento sulle misure di sicurezza in attuazione del Decreto Legislativo 30 giugno 2003, n. 196, dispone apposite misure per il caso in cui vengano affidati a terzi (ditte, privati o enti pubblici) i trattamenti di dati.

Tab. 5 – Trattamenti affidati all'esterno

Descrizione sintetica dell'attività esternalizzata	**Trattamenti di dati interessati**	**Soggetto esterno**	**Descrizione dei criteri e degli impegni assunti per l'adozione delle misure**
Scelta Revoca	Assistenza Sanitaria e gestione Esenzioni Redito / Patologia	CSI Piemonte	Convenzione Regionale
Registrazione ricette	Dati personali	CSI Piemonte	come da contratto in atto
Servizio di ossigenoterapia domiciliare e noleggio presidi per ventiloterapia domiciliare da nomenclatore tariffario delle protesi	Apertura pratica c/o sportelli ASL. Trasmissione a mezzo fax alla ditta di supporti cartacei recanti i dati personali e sensibili dei pazienti (nome e cognome, età, sesso, residenza/domicilio, diagnosi, programma terapeutico) per attivazione tempestiva servizio di fornitura o per aggiornamento dello stesso	MEDICAIR ITALIA s.r.l.	Assunzione impegno su base contrattuale. Obbligazione prevista in capitolato speciale di gara
Servizio di ossigenoterapia domiciliare	Apertura pratica c/o sportelli ASL. Trasmissione a mezzo fax alla ditta di supporti cartacei recanti i dati personali e sensibili dei pazienti (nome e cognome, età, sesso, residenza/domicilio, diagnosi, programma terapeutico) per attivazione tempestiva servizio di fornitura o per aggiornamento dello stesso	MEDIGAS ITALIA s.r.l.	Assunzione impegno su base contrattuale. Obbligazione prevista in capitolato speciale di gara.
Distribuzione apparecchi elettromedicali per funzionalità respiratoria, alimentare e microinfusione	Apertura pratica c/o sportelli ASL. Trasmissione a mezzo fax alla ditta di supporti cartacei recanti i dati personali e sensibili dei pazienti (nome e cognome, età, sesso, residenza/domicilio, diagnosi, programma terapeutico) per attivazione tempestiva servizio di fornitura o per aggiornamento dello stesso	VIVISOL S.r.l.	Assunzione impegno su base contrattuale. Obbligazione prevista in capitolato speciale di gara.
Servizio di distribuzione diretta domiciliare di presidi per incontinenti al domicilio e presso le strutture	Dati personali e sensibili. Apertura pratica c/o sportelli ASL. Trasmissione dei dati del paziente che opta per la distribuzione diretta	ARTSANA S.p.A.	Assunzione impegno su base contrattuale. Obbligazione

residenziali	(nome e cognome, età, sesso, residenza/domicilio, diagnosi, programma terapeutico) su supporto cartaceo al personale infermieristico della ditta per inserimento in programma distributivo		prevista in capitolato speciale di gara.
Servizio di registrazione ricette SSN, come da tracciato regionale, predisposizione estemporanea dati su richiesta enti istituzionali (NAS, Guardia di Finanza, Procure, Regione)	Ritiro ricette SSN a cura ditta ICS, registrazione ricette su supporto informatico, riconsegna ricette a Servizio Farmaceutico in scatole chiuse accompagnate da elaborati cartacei e DVD con caricamento su PC (in comodato d'uso con accesso protetto da password)	ICS CYBERNETIC & INFORMATIC SERVICE	Assunzione impegno su base contrattuale. Obbligazione prevista in capitolato speciale di gara.
Fornitura personalizzata vaccini sensibilizzanti	Trasmissione tramite fax o lettera cartacea in busta chiusa alla ditta di ordinativo del vaccino desensibilizzante con indicazione dei dati personali e sensibili dei pazienti	ALLERGY THERAPEUTICS s.r.l.; ALK-ABELLO' S.p.A.; ALLERGOPHARMA S.p.A.; ANALLERGO s.r.l.; LOFARMA S.p.A.; STALLERGENES ITALIA s.r.l.; SARM ALLERGOLOGIA E RICERCA; HAL ALLERGY s.r.l.	Secondo normativa vigente
Distribuzione ausili e presidi (lettini, carrozzine, girelli, ecc.)	Dati personali e sensibili	OFFICINA ORTOPEDICA FERRERO SRL - TORINO	Secondo normativa vigente

9. Cifratura dei dati o separazione dei dati identificativi

(Regola 19 punto 19.8)

I Dati Sensibili necessitano di modalità di gestione e protezione, quali cifratura e/o separazione fra i dati anagrafici identificativi e quelli atti a accertare lo stato di salute delle persone.
Sono altresì previsti l'adozione di criteri con i quali assicurare la sicurezza degli strumenti utilizzati per il trattamento degli stessi.

Tutti i fornitori esterni di software atto a gestire dati sensibili hanno adeguato le banche dati al fine di ottemperare quanto previsto dalla normativa vigente e di attestare per iscritto la conformità delle stesse.
La tabella seguente riporta la modalità di protezione adottata.

Trattamento	***Banca Dati***	***Ubicazione***	***Tecnica Adottata***	***Informazioni***
Assistenza Sanitaria;	UGSD00 SANITARIO UGSD00 CED	SC Sistema Informativo Tortona SOC Sistema	Separazione	

	LHA	Informativo Casale		
Gestione Amministrativa;	UAM CED2	SOC Sistema Informativo Casale		
Monitoraggio della spesa sanitaria; Analisi dei flussi di mobilità sanitaria attiva e passiva; Analisi dell'andamento della domanda e dell'offerta sanitaria	GIOVE CASSANDRA	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	Separazione	
Attività di Segreteria e Protocollo; Gestione di rapporti di lavoro e collaborazioni varie.	ATTIUNICI	SOC Sistema Informativo Casale		
Erogazione competenze mensili ai dipendenti; Liquidazione compenso per titolari di incarichi e collaborazioni; Rilascio CUD; Effettuazione trattenute di legge; Gestione politiche del personale; Formazione professionale.	WHR	SC Sistema Informativo Tortona	Separazione	
Affitti attivi e passivi; Alienazioni di beni patrimoniali; Gestione patrimonio mobiliare i immobiliare; Anagrafi clienti e fornitori; Fatturazione attiva di prestazioni sanitarie istituzionali e di libera professione; Interrogazione banche dati Equitalia/Enti previdenziali e Assicurativi; Cessioni quinto stipendio/ ritenute sindacali/pignoramenti stipendi.	UAE CED2 Archivi Informatica Individuale	SOC Sistema Informativo Casale Altre sedi	Separazione	
Attività connesse al settore assicurativo; Attività connesse al contenzioso amministrativo; Attività connesse al recupero crediti;	Archivi Informatica Individuale	S.C. Ufficio Legale, Settore Gestione Assicurazioni e Consulenza – sede di Novi Ligure, Ovada, Settore Gestione Contenzioso Amministrativo e Recupero Crediti Sede di Casale Monferrato	/	
Fornitura di beni o servizi; Attività commerciali;	UAE CED2	SOC Sistema Informativo Casale	/	
Schede cliniche informatizzate	MedOffice GA	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	Separazione	
Diagnosi dei pazienti strumenti radiologici	SYNAPSE	SC Sistema Informativo Tortona SOC Sistema Informativo Casale SC Informatica Novi	Separazione	
Prenotazione e refertazione di esami clinici o visite specialistiche per via telematica o telefonica	TELECUP	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	Separazione	
Diagnosi dei pazienti strumenti Laboratorio Analisi	METAFORA GELAB	SC Sistema Informativo Tortona	Separazione	

		SOC Sistema Informativo Casale SC Informatica Novi		
Sorveglianza sanitaria per la tutela della salute pubblica; Indagine epidemiologica; Interventi in caso di calamità, epidemie o malattie infettive; Prevenzione; Ricerca medica e biomedica; Rilevazione di malattie infettive o diffusive;	EPIDEM	SC Epidemiologia	Separazione	
Prevenzione infortuni; Tutela salute e sicurezza dei lavoratori; Analisi dell'uso di merce in distribuzione o in commercio; Difesa del suolo, igiene urbana o tutela dell'ambiente; Prevenzione, accertamento e repressione di reati;	Archivi Informatica Individuale	IGIENE PUBBLICA	Separazione	
Mappatura delle strutture in cui sono detenuti animali; Vigilanza sul commercio di animali; Aggiornamento delle anagrafi zootecniche.	ARVET	SC Sistema Informativo Tortona SOC Sistema Informativo Casale SC Informatica Novi Regione Piemonte	Separazione	
Accertamento stato invalidità civile, cecità, sordomutismo, handicap; Per relazioni su cause relative a decessi richieste dall'autorità giudiziaria; Esenzioni ticket per patologia; Assistenza sanitaria; Legge 210/1992.	UGSD00 SANITARIO UGSD00 CED	SC Sistema Informativo Tortona SOC Sistema Informativo Casale	Separazione	

10. Strumenti Elettronici

Tutti i sistemi di elaborazione di categoria server in uso in azienda adottano almeno le seguenti caratteristiche:

- tutte le aree di memoria su disco magnetico destinate a contenere i dati sono tutelate da misure di ridondanza - con tecniche almeno di mirroring per i dischi del SO, RAID livello 5 per i dischi dei dati
- ogni server possiede sistema di backup dei dati e delle configurazioni attraverso un sistema di backup di adeguate dimensioni e velocità - unità di backup. Nel caso dei sistemi presenti nei locali del CED Aziendale ogni server dispone anche di un sistema di backup centralizzato (Tivoli Storage Manager), come dettagliata nella scheda dei server aziendali
- Come dettagliato nella scheda dei server i sistemi con il livello di rischio maggiore adottano funzionalità "Multi-Homed" con doppia scheda di rete in grado di resistere a guasti singoli
- Per ogni server è disponibile una scheda nella quale deve essere obbligatoriamente indicato dove è possibile trovare copia delle informazioni per l'accesso - USERID e PASSWORD del super utente - per manovre di emergenza sull'elaboratore. Tali informazioni sono conservate in luogo presidiato e sotto chiave.

10.1 Regole di buon uso del sistema informatico aziendale

Vengono qui richiamate alcune proibizioni e alcuni obblighi che il dipendente ha nell'uso della infrastruttura informatica aziendale e più in generale nella fruizione del sistema informativo dell'azienda.

10.1.1 Crimine informatico e tutela del diritto d'autore

Vista la legge n. 128 del 21.05.2004 relativa alla tutela del diritto d'autore è vietata la riproduzione o la duplicazione con qualsiasi mezzo e a qualsiasi titolo dei programmi informatici e dei manuali a corredo dei programmi, si ricorda infatti che anche i manuali sono coperti dalla legge sul diritto di autore e possono essere riprodotti solo dietro autorizzazione del titolare dei diritti esclusivi. Il Servizio Informativo Aziendale, qualora tecnicamente possibile deve predisporre copie di riserva dei programmi dotati di regolare licenza allo scopo di prevenire accidentali perdite dell'originale e quindi danni patrimoniali all'azienda. Tale copia di riserva potrà essere usata soltanto per ripristinare le funzionalità del programma, quando non sia possibile utilizzare il programma originale.

10.1.2 Tutela dei dati memorizzati sulle stazioni di lavoro personale e reimpiego dei supporti di memorizzazione

L'azienda persegue una politica di centralizzazione nella gestione dei dati aziendali, per cui progressivamente le gestioni locali di dati scompariranno sostituite da gestioni centralizzate su server. Fino a che questo processo non sarà stato portato a compimento potranno esistere gestioni locali di dati su stazioni di lavoro personali - personal computer non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati – la cui tutela è demandata all'utente finale. L'effettuazione dei salvataggi con frequenza opportuna – almeno comunque settimanale - su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo - possibilmente sotto chiave e in contenitori ignifughi - è compito del singolo dipendente che usa la stazione nel caso di stazioni di lavoro usate da un solo utilizzatore, da un incaricato opportunamente individuato dal responsabile del trattamento nel caso di stazioni di lavoro condivise.
È vietato l'uso di supporti di memorizzazione removibili per la memorizzazione di dati personali o sensibili.

10.1.3 Buon uso della rete di comunicazione

La rete di trasmissione dati e fonia è un prezioso bene aziendale condiviso e pertanto va gestita nel rispetto delle esigenze complessive di azienda. In funzione di ciò viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Sistema Informativo Aziendale. È altresì vietato alterare in qualsiasi modo la configurazione software della stazione di lavoro - o di altri dispositivi direttamente connessi alla rete, dati o fonia - per quanto attiene all'accesso alla rete. È anche fatto divieto di utilizzare in qualsiasi modo la rete aziendale per fini non espressamente autorizzati. In particolare tali divieti si possono tradurre, anche se non esaurire, nelle seguenti esplicite proibizioni:

- divieto di condividere cartelle in rete (né dotate di password, né sprovviste di password)
- divieto di alterare la configurazione delle configurazioni di rete di stazioni di lavoro e altri dispositivi in rete (stampanti condivise, ecc…), comprendendo in ciò anche il divieto di aggiungere protocolli di rete o servizi in rete (per es. condivisione di stampanti in rete, browsing di risorse di rete, ecc…)
- divieto di monitorare ciò che transita in rete.

È inoltre vietata l'installazione non autorizzata di Modem per linee analogiche o digitali che sfruttino il sistema di comunicazione in fonia per l'accesso a banche dati esterne o interne all'azienda.

È vietata l'installazione di hardware o software di qualsiasi tipo che consenta o faciliti il *by pass* delle misure di presidio del confine aziendale - per es. software di comunicazione che garantiscano accessi che non passino dai Firewall Aziendali o dagli altri accessi autorizzati e presidiati.

Al fine di proteggere la rete Aziendale da siti internet che potrebbero pregiudicarne la sicurezza e per salvaguardare il rischio di utilizzi impropri della rete vengono adottate una serie di misure tecnologiche e organizzative per prevenire queste possibilità, attraverso l'adozione di hardware in grado di effettuare analisi preventive (ed anonime) del contenuto della navigazione e del contenuto dei messaggi di posta elettronica. Tali misure individuano preventivamente i siti considerati correlati o meno con la prestazione lavorativa; utilizzano filtri che prevengono determinate operazioni, quali l'accesso a siti inseriti in una black list o il download di file musicali o multimediali coperti da diritto d'autore.

Per quanto riguarda la posta elettronica, tutti i messaggi contenenti elementi virali o classificati come SPAM non saranno inoltrati alla rete aziendale.

10.1.4 Doveri connessi alla corretta conservazione delle parole chiave di accesso

L'utente inoltre è tenuto a conservare nella massima segretezza la parola di accesso ai sistemi e qualsiasi altra informazione legata al processo di autenticazione.
Inoltre l'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro, o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (per es. perché impegnato in compiti che richiedono totalmente la sua attenzione). Occorre prestare anche particolare attenzione alle stampe prodotte con sistemi informatizzati: la produzione dei documenti deve essere presidiata o collocata in locali ad accesso controllato.

E' compito dei responsabili delle Strutture Semplici e Complesse un costante e meticoloso controllo al fine di arginare pratiche che la normativa identifica come veri e propri crimini informatici e causa di costi sempre crescenti indotti da un cattivo uso delle attrezzature stesse.

I responsabili delle varie articolazioni organizzative, di concerto con il Sistema Informativo Aziendale, dovranno adottare gli atti e le misure necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione dell'azienda.

10.1.5 Regolamento Aziendale per l'utilizzo delle postazioni di Informatica individuale

Ad integrazione di quanto riportato nei capitoli precedente l'ASL AL adotta inoltre uno specifico regolamento per l'utilizzo delle postazioni di Informatica individuale per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.
Il Regolamento aziendale (ALLEGATO D) viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta l'Azienda.

10.2 I virus Informatici – malicious code.

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

1. si dotano tutte le attrezzature di confine di un adeguato software antivirale e si stabilisce l'aggiornamento delle firme almeno in ragione giornaliera.
2. si dota di software antivirale - e predispongono adeguati meccanismi per mantenere tale software aggiornato ogni client aziendale
3. si dotano di software antivirale tutti i file server all'interno del confine aziendale per la scansione dei documenti gestiti. Vedi Elenco dei file server paragrafo precedente.
4. per quanto possibile si dovranno configurare i profili abilitativi di tutti gli utenti aziendali con privilegi che non consentano l'installazione o l'esecuzione di programmi non autorizzati sia sulle macchine client che sui server
5. per quanto organizzativamente possibile ed appropriato, dovranno essere disabilitate sui server le funzionalità di editor e di file transfer.

Si invitano inoltre gli utenti:

- alla massima cautela nella gestione dei supporti magnetici e della posta elettronica: in particolare ogni qualvolta un supporto di memorizzazione - dischetto removibile, nastro magnetico, disco magneto-ottico e ogni altro supporto di memorizzazione removibile - sia stato utilizzato su un computer diverso dal proprio - supponendo che il proprio PC sia immune da infezioni - occorrerà verificare l'assenza di virus mediante un programma antivirale aggiornato. Se non vi è l'assoluta certezza che il proprio computer possieda un antivirus aggiornato non sarà possibile utilizzare il supporto di memorizzazione - in quanto potenzialmente infetto.
- in generale sarebbe bene conoscere sempre con precisione quale sia la fonte dei dati, ed essere certi che tale fonte sia affidabile e sicura; è preferibile non utilizzare un supporto di memorizzazione removibile di cui non si conosca la fonte
- è bene sempre evitare di leggere o utilizzare allegati di messaggi di posta elettronica che non provengano da fonti certe, riconosciute e sicure; nel caso pervenga un messaggio di tale natura procedere immediatamente alla eliminazione. Nel caso si abbia il sospetto che il proprio sistema di elaborazione sia stato infettato avvertire il personale tecnico competente e non operare per alcun motivo scambio di supporti di memorizzazione o posta elettronica con altri.

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

L'azienda possiede sottosistemi che fanno uso di supporti ottici per la memorizzazione dei dati, quelli che debbono essere conformi alla deliberazione 42/2001**.**

ALLEGATO A

COMPITI DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

- Attivare ed istruire il procedimento per l'effettuazione delle notificazioni di inizio trattamento, di rettifica e di fine trattamento (in caso di cessazione del trattamento dei dati e delle eventuali operazioni di distruzione nonché in caso di cessione dei dati personali).

- Curare l'effettuazione delle informative scritte all'interessato, nei casi prescritti dal D.Lgs. n. 196/03.

- Curare la raccolta del consenso dell'interessato, nelle forme prescritte dal D.Lgs. n. 196/03.

- Fornire la risposta all'interessato circa l'esistenza o meno di dati personali che lo riguardano, la comunicazione in forma intelligibile degli stessi, della loro origine, delle finalità del trattamento e della logica su cui esso si basa.

- Disporre la cancellazione, la trasformazione in forma anonima, il blocco, l'aggiornamento, la rettificazione o l'integrazione dei dati quando prescritto e darne conoscenza a coloro cui i dati sono stati comunicati o diffusi.

- Identificare tutti gli archivi presenti su server di rete, su personal computer, su supporti magnetici, ottici, cartacei, ecc..

- Inventariare i trattamenti in corso.

- Definire per ciascun archivio contenente dati personali la durata del trattamento nominativo (non superiore a quella necessaria alle finalità per cui sono stati raccolti o successivamente trattati).

- Verificare/attivare procedure di cancellazione dei dati obsoleti.

- Verificare/attivare procedure per la distruzione di archivi non informatici superati.

- Verificare/attivare procedure di salvataggio atte a garantire l'integrità degli archivi per tutta la durata del trattamento.

- Attuare una efficace protezione fisica degli archivi (conservazione dei dati in locali riservati e con accesso controllato all'interno di armadi chiusi a chiave).

- Porre in essere misure di interdizione di accessi non autorizzati attraverso l'autenticazione dell'utente (mediante l'utilizzo di

dispositivi fisici di riconoscimento -badge- o l'uso di password di riconoscimento da formare attraverso la scelta di elementi identificativi non usuali e ragionevolmente complessi, da cambiare spesso e da non divulgare).

- Individuare chi deve operare sui dati distinguendo tra personale interno (dipendente dal titolare).

- Conferire eventuali incarichi scritti a compiere le operazioni del trattamento, e fornire le relative istruzioni.

- Informare efficacemente gli incaricati del trattamento sulle procedure da seguire ai fini del perseguimento della riservatezza, della sicurezza di accesso agli archivi, della integrità dei dati ed effettuare il monitoraggio sull'osservanza da parte dell'incaricato delle istruzioni impartite.

- Comunicare anche ai non addetti al trattamento il divieto di creare archivi contenenti dati personali senza la preventiva autorizzazione del responsabile. Successivamente monitorare gli effetti della comunicazione.

- Verificare le procedure di accesso fisico e logico agli elaboratori.

- Per l'utilizzo delle procedure informatizzate in rete aziendale occorre comunicare per iscritto al Servizio Informativo Aziendale l'avvenuta assegnazione di autorizzazioni di accesso ai trattamenti da parte dei propri incaricati. Anche nel caso in cui all'incaricato venissero a mancare le credenziali per l'accesso ai trattamenti informatizzati, sarà cura del responsabile del trattamento chiederne la disattivazione al Sistema Informativo.
  È individuato un modulo di "Concessione-revoca-modifica" delle abilitazioni applicative che i responsabili utilizzeranno per le comunicazioni del caso al Servizio Informativo Aziendale.

- Adottare tutte le misure minime di sicurezza di cui al Regolamento sulle misure di sicurezza.

ALLEGATO B

ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

1) CONSERVAZIONE DI BANCHE DATI PERSONALI

1. I dati devono essere conservati in luoghi sicuri, con accesso protetto:
   - sarà opportuno assicurarsi che l'ufficio in cui sono conservate le banche dati sia sempre custodito durante l'orario di apertura;
   - fuori orario di apertura o comunque in assenza di incaricati:
     - le banche dati dovranno essere custodite in armadi chiusi a chiave ovvero, in mancanza di serratura, dovrà essere chiuso a chiave lo stesso locale adibito ad archivio;
     - il P.C. su cui sono memorizzate le banche dati dovrà essere spento e, ove non sia possibile la chiusura dello sportellino di accensione dello stesso ovvero non sia prevista una password di accesso al programma , dovrà essere chiuso a chiave il locale ove è ubicato il P.C.;
   - le chiavi degli armadi, dei locali ovvero dei P.C. ove sono custodite la banche dati devono essere depositate in luogo sicuro; una copia di dette chiavi dovrà essere custodita dal responsabile dell'ufficio;
   - la password di accesso al programma:
     - non deve essere comunicata ad alcuno, salvo che al responsabile del trattamento, ove nominato;
     - in caso di assenza od impedimento dell'incaricato, potrà essere nota ad un sostituto, previa comunicazione al responsabile del trattamento;
     - non deve essere scritta su agende o altri supporti cartacei conservati nell'ufficio ove è installato il P.C.;
     - dovrà essere digitata al riparo di sguardi indiscreti;
     - non deve essere banale o facilmente individuabile.

2. I supporti (cartacei) per la memorizzazione di "dati sensibili" devono recare indicazioni in ordine al nome dell'incaricato del trattamento dei dati, ai dati contenuti ed al periodo di riferimento.

   2.1 E' vietato l'uso di supporti removibili per la memorizzazione di dati personali o sensibili.

2) COMUNICAZIONE DI DATI PERSONALI

1. Comunicazione tra uffici dell'Azienda: occorre trasmettere i soli dati necessari alle finalità per cui sono stati richiesti (ad esempio sarà inutile indicare il nominativo del paziente

visitato dal consulente quando il dato necessario ai fini della fatturazione è solo il numero degli accessi del consulente).

2. Comunicazione al di fuori dell'Azienda: la comunicazione di dati al di fuori dell'Azienda deve essere autorizzata dal responsabile del trattamento dei dati.

3. La trasmissione e la comunicazione di "dati sensibili" mediante posta, all'interno o all'esterno dell'Azienda, dovrà avvenire sempre mediante supporti (cartacei, ...) confezionati in buste o pacchi chiusi. Nel caso di "dati personali sensibili", sulla confezione o su un documento accompagnatorio , deve essere indicata la dicitura DATI RISERVATI.

   3.1 Utilizzo posta elettronica interna per dati sensibili in maniera anonima, ovvero tale da non permettere l'identificazione dei soggetti.

   3.2 La trasmissione e la comunicazione di "dati sensibili" mediante l'utilizzo di posta elettronica esterna all'Azienda potrà essere utilizzata solo dopo aver reso illeggibile il documento attraverso strumenti di cifratura.

4. Onde evitare accessi impropri ai dati personali è opportuno elaborare gli stessi al riparo da sguardi indiscreti, soprattutto allorché si tratti di dati aventi carattere strettamente personale(ad esempio dati inerenti alla salute).

5. La distruzione di documenti contenenti dati aventi carattere strettamente personale dovrà avvenire in modo da rendere illeggibile il documento stesso.

6. Si rammenta, in proposito, il disposto dell'art. 15 del D.P.R. 10 gennaio 1957 n. 3 "Statuto degli impiegati civili dello Stato", che recita:
   "L'impiegato deve mantenere il segreto d'ufficio. Non può trasmettere a chi non ne abbia diritto informazioni riguardanti provvedimenti od operazioni amministrative, in corso o concluse, ovvero notizie di cui sia venuto a conoscenza a causa delle sue funzioni, al di fuori delle ipotesi e delle modalità previste dalle norme sul diritto di accesso. Nell'ambito delle proprie attribuzioni, l'impiegato preposto ad un ufficio rilascia copie ed estratti di atti e documenti nei casi non vietati dall'ordinamento".

3) CREAZIONE DI BANCHE DATI

1. La creazione di banche dati deve essere autorizzata dal responsabile del servizio. La gestione di tali banche dati potrà avvenire in modalità informatizzata a condizione che gli archivi vengano gestiti centralmente sui server aziendali e non sulle singole stazioni informatiche locali.

4) MISURE DI SICUREZZA

1. Gli incaricati dovranno attenersi a quanto disposto con il Regolamento sulle misure di sicurezza di cui all'allegato C del Documento Programmatico sulla Sicurezza.

ALLEGATO C

REGOLAMENTO SULLE MISURE DI SICUREZZA IN ATTUAZIONE DEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

CAPO I

PRINCIPI GENERALI

Art. 1
Misure di sicurezza

In ottemperanza a quanto previsto dal D.Lg.vo 30 giugno 2003, n. 196, sono individuate, con il presente Regolamento, le misure di sicurezza per il trattamento dei dati personali, ai sensi degli artt. 33 e seguenti nonché dell'allegato B del succitato Decreto.

Art. 2
Finalità delle Misure di Sicurezza

Le misure di sicurezza di cui al presente regolamento hanno lo scopo di assicurare un livello minimo di protezione dei dati personali nonché di:

- Evitare la distruzione o perdita anche accidentale dei dati
- Evitare gli accessi non autorizzati
- Evitare trattamenti non consentiti

Art. 3
Misure di sicurezza minime

Tutti i responsabili e gli incaricati dei dati devono scrupolosamente attenersi alle seguenti misure minime:

- I dati devono essere conservati in luoghi sicuri, con accesso protetto, meglio ancora con accesso regolamentato. L'ufficio in cui si sono conservate le banche dati deve sempre essere custodito durante l'orario di apertura.
- Si deve controllare e vigilare affinché i dati vengano trattati/utilizzati esclusivamente per gli scopi e con le modalità stabilite da norme di legge o da regolamenti interni.
- La comunicazione tra uffici dell'Azienda deve contenere i soli dati necessari alle finalità per cui sono stati richiesti.
- La trasmissione e la comunicazione di "dati personali" mediante posta, all'interno o all'esterno dell'Azienda, deve avvenire sempre mediante supporti cartacei confezionati in buste o pacchi chiusi, se affidati a persone non autorizzate all'accesso.

- E' indispensabile adottare tutte le misure necessarie affinché i documenti contenenti "dati sensibili" siano accessibili solo dalle persone autorizzate.
- Onde evitare accessi impropri ai dati personali, è opportuno comunicare e/o trattare gli stessi al riparo da sguardi indiscreti, anche prevedendo eventuali distanziatori, soprattutto se in relazione a "dati sensibili", con particolare riferimento agli sportelli, uffici, ambulatori aziendali, etc..
- E' vietato trasmettere documenti contenenti "dati sensibili" tramite Internet.
- La distruzione di documenti contenenti "dati personali" o "dati sensibili" deve avvenire in modo da rendere illeggibile il documento stesso.
- Fuori orario di apertura o, comunque, in assenza di incaricati:
  - le banche dati, se su supporto cartaceo o informatico, dovranno essere custodite in armadi chiusi a chiave ovvero, in mancanza di serratura, dovrà essere chiuso a chiave lo stesso locale adibito ad archivio;
  - le chiavi degli armadi, dei locali, ovvero degli strumenti informatici ove sono custodite le banche dati devono essere depositate in luogo sicuro; una copia di dette chiavi dovrà essere custodita dal Responsabile dell'ufficio o dal suo delegato.

CAPO II

MISURE DI SICUREZZA MINIME PER TRATTAMENTI EFFETTUATI CON STRUMENTI NON AUTOMATIZZATI

Art. 4
Trattamento dei dati personali

- L'accesso degli incaricati del trattamento deve essere limitato ai soli dati necessari all'adempimento dei compiti loro assegnati. Agli stessi sono impartite istruzioni scritte finalizzate al controllo e alla custodia per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento degli atti e dei documenti contenenti dati personali.
- Gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere conservati dagli stessi in maniera che ad essi non accedano persone prive di autorizzazione e restituiti al termine delle operazioni affidate.
- Nel trattamento di dati sensibili e giudiziari devono essere osservate le seguenti ulteriori modalità:
  a) i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di "dati sensibili" e "dati giudiziari", se affidati agli incaricati del

trattamento, devono essere conservati, fino alla restituzione, in contenitori muniti di serratura.

b) L'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

- La conservazione e la riproduzione della documentazione relativa al trattamento dei dati sensibili dovrà avvenire, comunque, secondo le modalità previste dalle misure adottate per la tutela degli stessi.
- Qualora gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura sono identificate e registrate.

CAPO III

ACCESSO E CONSERVAZIONE DI BANCHE DATI PERSONALI DI ORGANI INTERNI

Art. 5
Collegio Sindacale

I componenti del Collegio Sindacale possono accedere a dati personali di cui è titolare l'A.S.L. AL, nell'osservanza delle seguenti disposizioni:

- Attività espletata presso la sede dell'Azienda:
  - le banche dati vengono messe a disposizione da dipendenti dell'Azienda: i componenti del Collegio possono, tramite i responsabili dei Servizi competenti, entrare in possesso di chiavi di accesso agli uffici, degli armadi ove sono custodite le banche dati e avere accesso agli archivi informatici nonché conoscere la password di accesso ai medesimi;
  - i supporti magnetici o cartacei per la memorizzazione di "dati sensibili", elaborati dai componenti del Collegio, devono recare indicazioni in ordine al nome dell'incaricato del trattamento dei dati, ai dati contenuti ed al periodo di riferimento;
- Attività svolta presso altra sede:
  - i dati devono essere custoditi in luogo sicuro con accesso protetto;
  - i supporti (magnetici o cartacei) per la memorizzazione di "dati sensibili" devono recare indicazioni in ordine al nome del titolare dei Responsabili ove nominati e dell'incaricato del trattamento dei dati, nonché in ordine ai dati contenuti ed al periodo di riferimento.

CAPO IV

MISURE DI SICUREZZA DA RICHIEDERE NEL CASO DI AFFIDAMENTO DI ELABORAZIONE DATI A DITTE ESTERNE

Art. 6
Misure per affidamento a terzi

Nel caso in cui vengano affidati a terzi (ditte, privati o enti pubblici) i trattamenti dei dati in questione, devono essere garantite le seguenti misure di sicurezza:

- I "dati personali" sensibili trattati e/o conservati dovranno riportare la dicitura "dati riservati";
- Nel caso si utilizzino supporti magnetici o equivalenti, il supporto deve essere etichettato in modo tale da evidenziare il nome della società proprietaria dei dati, il nome della società che lo ha prodotto (nel caso in cui differisca dalla società proprietaria dei dati), i dati contenuti ed il periodo di riferimento. Le stesse informazioni devono essere riportate come intestazioni, nel caso in cui i "dati personali" siano riportati su un supporto cartaceo (ad es. tabulato);
- L'accesso ai dati deve essere protetto con codici di accesso e parole chiave costituite da almeno 8 caratteri alfanumerici oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed e' modificata da quest'ultimo al primo utilizzo e successivamente.
- Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
- Quando l'accesso ai dati e agli strumenti elettronici e' consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali e' organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali

devono informare tempestivamente l'incaricato dell'intervento effettuato.

- Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.
- Occorre adottare le misure opportune al fine di garantire che i supporti informatici utilizzati siano esenti da virus.

Art. 7
Disposizioni finali

Le misure contenute nel presente Regolamento dovranno essere rispettate anche da consulenti, liberi professionisti, Compagnie di Assicurazione, da società, etc., che in qualunque modo abbiano a trattare i dati in questione.

Regolamento Aziendale per l'utilizzo delle postazioni di Informatica individuale

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'ASL AL ai rischi di un coinvolgimento sia patrimoniale che penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso che l'utilizzo delle risorse informatiche e telematiche Aziendali deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, l'ASL AL ha adottato il presente regolamento, promosso dal Sistema Informativo, alla luce del "Piano programmatico Aziendale sulla sicurezza informatica", per contribuire alla massima diffusione della cultura della sicurezza ed evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.

Il Regolamento aziendale di seguito riportato viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta l'Azienda.

1 Utilizzo del Personal Computer

1.1 Il Personal Computer affidato al dipendente è **uno strumento di lavoro**
Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione
Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza

1.2 Non è consentita l'attivazione della password d'accensione (bios), senza preventiva autorizzazione da parte della SOC. Sistema Informativo

1.3 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sul proprio PC, salvo previa autorizzazione esplicita da parte del personale della SOC. Sistema Informativo

1.4 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio

1.5 Le informazioni archiviate informaticamente devono essere esclusivamente quelle previste dalla legge o necessarie all'attività lavorativa

1.6 Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante

1.7 La tutela della gestione locale di dati su stazioni di lavoro personali - personal computer che gestiscono localmente documenti e/o dati - è demandata all'utente finale che dovrà effettuare, con frequenza opportuna, i salvataggi su supporti magnetici e/o di rete e la conservazione degli stessi in luogo idoneo. E' comunque vietato l'uso di supporti di archiviazione removibili per la

memorizzazione dei dati sensibili

1.8 Le gestioni locali dei dati dovranno scomparire per essere sostituite da gestioni centralizzate su server

1.9 Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Sistema Informativo Aziendale

1.10 Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi delle Legge n.128 del 21.05.2004

1.11 Gli operatori del Sistema Informativo possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

2. Utilizzo della rete dell'ASL AL

2.1 L'accesso alla rete aziendale è protetto da password; per l'accesso deve essere utilizzato il proprio profilo personale

2.2 E' fatto divieto di utilizzare la rete aziendale per fini non espressamente autorizzati

2.3 E' vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del Sistema Informativo Aziendale

2.4 E' vietato condividere cartelle in rete (né dotate di password, né sprovviste di password)

2.5 E' vietato monitorare ciò che transita in rete

2.6 E' vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonico per l'accesso a banche dati esterne o interne all'azienda.

3. Gestione delle Password

3.1 Le password d'ingresso alla rete, di accesso ai vari programmi in rete per i trattamenti dei dati e ad Internet, sono attribuite dalla SOC. Sistema Informativo. Al riguardo è individuato un modulo di "Concessione/Revoca/Modifica abilitazioni applicative" che i responsabili dei trattamenti utilizzeranno per le comunicazioni del caso alla SOC. Sistema Informativo

3.2 L'utente è tenuto a conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione

3.3 L'utente è tenuto a scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso

3.4 La password deve essere immediatamente sostituita, dandone comunicazione alla SOC. Sistema Informativo, nel caso si sospetti che la stessa abbia perso la segretezza.

4. Utilizzo di PC portatili

4.1 L'utente è responsabile del PC portatile assegnatogli dall'Azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

4.2 Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna

4.3 I PC portatili utilizzati all'esterno (convegni, visite in azienda), in caso di allontanamento, devono essere custoditi in un luogo protetto

4.4 II portatile non deve essere mai lasciato incustodito e sul disco devono essere conservati solo i files strettamente necessari

4.5 Nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server)/Accesso Remoto:

- utilizzare l'accesso in forma esclusivamente personale
- utilizzare la password in modo rigoroso

4.6 Disconnettersi dal sistema RAS al termine della sessione di lavoro

4.7 Collegarsi periodicamente alla rete interna per consentire il caricamento dell'aggiornamento dell'anti virus

4.8 Non utilizzare abbonamenti Internet privati per collegamenti alla rete.

5. Uso della posta elettronica

5.1 L'abilitazione alla posta elettronica deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa al Sistema Informativo

5.2 La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse

5.3 Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli

5.4 Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .**pif** .bat .cmd), questi ultimi non devono essere aperti

5.4 Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta

5.5 Utilizzare, nel caso di invio di allegati pesanti, i formati compressi (*.zip *.jpg)

5.6 Nel caso in cui si debba inviare un documento all'esterno dell' Azienda è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf). Tale software specifico è fornito dal Ced previa richiesta

5.7 L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali Prima di iscriversi occorre verificare in anticipo se il sito è affidabile

5.8 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti

5.9 Per la trasmissione di file all'interno dell'asl20 è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati che non devono

mai superare i 5 MB.

5.10 E' obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

6. Uso della rete Internet e dei relativi servizi

6.1 L'abilitazione alla posta esterna e ad Internet deve essere preceduta da regolare richiesta del Responsabile di funzione/unità organizzativa al Sistema Informativo

6.2 Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa

6.3 E' assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa

6.4 non possono essere utilizzati modem privati per il collegamento alla rete

6.5 E' fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dalla SOC. Sistema
Informativo.

6.6 E' vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati),di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

7 Protezione antivirus

7.1 Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc..)

7.2 Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus aziendale

7.3 Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l' utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer
- segnalare l'accaduto alla SOC. Sistema Informativo

7.4 Ogni dispositivo magnetico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato

8 Osservanza delle disposizioni in materia di Privacy

8.1 E' obbligatorio attenersi alle disposizioni di cui al Regolamento sulle misure minime di sicurezza e al Documento di Programmazione e sicurezza di cui

alle Deliberazioni 30.06.2004 n. 571 e 05.08.2004 n. 679 visualizzabili nel sito Internet dell' Azienda www.aslal.it nell'area riservata sezione Sistema Informativo.

9 Non osservanza della normativa aziendale

9.1 Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

10 Aggiornamento e revisione

10.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento tramite comunicazione alla SOC. Sistema Informativo.

10.2 Il presente Regolamento è soggetto a revisione con frequenza annuale.