UNITÁ LOCALE SOCIO-SANITARIA n°3

Via dei Lotti, 40
36061 Bassano del Grappa (Vi)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento è predisposto in attuazione del punto 19 del

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

del

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
***(*Decreto legislativo 30 giugno 2003, n. 196)**

Rev.	Data	Descrizione	Redatto	Verificato	Approvato
	31/03/10	Revisione annuale			

Indice del documento

1. SCOPO

Il presente Documento Programmatico Sulla Sicurezza è adottato, in base alle disposizioni di cui al punto 19 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (nel seguito denominato più semplicemente DISCIPLINARE TECNICO) del CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (nel seguito denominato più semplicemente CODICE), per definire le politiche di sicurezza in materia di trattamento di dati personali, ed i criteri organizzativi per la loro attuazione.

In particolare nel Documento Programmatico Sulla Sicurezza vengono definiti i criteri tecnici e organizzativi per:

a) la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
b) i criteri e le procedure per assicurare l'integrità dei dati;
c) i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

2. CAMPO DI APPLICAZIONE

Il Documento Programmatico Sulla Sicurezza, in raccordo con il Decreto legislativo 30 giugno 2003 n. 196, adottato dall'AZIENDA SANITARIA ULSS N°3, e del quale si richiamano tutte le definizioni e disposizioni, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Identificativi

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali 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 tutti gli Uffici dell'AZIENDA SANITARIA ULSS N°3.

3. PRINCIPALI RIFERIMENTI LEGISLATIVI E COMUNICAZIONI AZIENDALI

- CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (Gazzetta Ufficiale 29 luglio 2003, n. 174 - Supplemento ordinario n. 123/L)
- DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Allegato B)

Al fine di recepire completamente lo spirito con cui è stato varato il CODICE, l'AZIENDA SANITARIA ULSS N°3 ha elaborato il seguente Documento Programmatico Sulla Sicurezza (nel seguito denominato più semplicemente DPSS).

Si richiama la deliberazione n. 1504 del 21.12.2005, con la quale è stato aggiornato il regolamento per l'uso di postazioni multimediali per la navigazione in Internet.

4. COMPOSIZIONE DEL DOCUMENTO

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un Documento Programmatico Sulla Sicurezza contenente idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- 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;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- 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;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Il Documento Programmatico Sulla Sicurezza elaborato dall'AZIENDA SANITARIA ULSS N°3 testimonia lo sforzo fatto dall'AZIENDA SANITARIA ULSS N°3 al fine di garantire la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.

Nel documento vengono identificate le **risorse da proteggere** che hanno impatti con i problemi di sicurezza e svolgono un ruolo significativo nei processi di trattamento dei dati personali. L**'analisi dei Rischi** costituisce un punto fondamentale per affrontare in maniera definita e controllata le problematiche di sicurezza; rappresenta l'attività di raccolta ed analisi delle debolezze e lacune del rispetto del Codice in azienda.
Sono state poi definite le **misure di sicurezza** (organizzative, fisiche e logiche), in essere e da adottare, per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.
Vengono successivamente elencati **i criteri e le modalità per il ripristino dei dati** in caso di perdita dei dati dovuta, ad esempio, ad un guasto.
E' iniziata 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.

5. ORGANIZZAZIONE DELL'AZIENDA

5.1 DESCRIZIONE DELL'AZIENDA

L'AZIENDA SANITARIA ULSS N°3 è un'azienda pubblica che eroga servizi sanitari.
Il Decreto Legislativo 502/92 e successive integrazioni e modificazioni, qualifica le Unità Sanitarie Locali costituite in aziende pubbliche come enti strumentali della Regione per assicurare i livelli essenziali ed uniformi di assistenza, definiti dal Piano Sanitario Nazionale nel rispetto dei principi di cui all'art. 1, comma 2 del predetto decreto legislativo, finalizzati alla tutela della salute della popolazione.

L'AZIENDA SANITARIA ULSS N°3 ha il compito di assicurare l'erogazione dei livelli essenziali ed uniformi di assistenza previsti dal Piano Sanitario Nazionale e di realizzare, nel proprio ambito territoriale, le finalità del Servizio Socio-Sanitario Regionale, impiegando nel processo di assistenza le risorse ad essa assegnate in modo efficiente, oltre che efficace ed economico.
I valori che ispirano l'azione dell'Azienda sono la promozione e la tutela della salute, quale bene collettivo ed individuale e l'equità di accesso dei cittadini ai servizi socio-sanitari da essa gestiti.

La sede legale dell'Azienda Sanitaria U.L.S.S. n. 3, è fissata a Bassano del Grappa (VI) - Via dei Lotti, 40.

L'ambito territoriale dell'Azienda Sanitaria U.L.S.S. n. 3 comprende n. 28 Comuni:

Asiago	Mussolente
Bassano del Grappa	Nove
Campolongo sul Brenta	Pianezze
Cartigliano	Pove del Grappa
Cassola	Roana
Cismon del Grappa	Romano d'Ezzelino
Conco	Rosà
Enego	Rossano Veneto
Foza	Rotzo
Gallio	San Nazario
Lusiana	Schiavon
Marostica	Solagna
Mason Vicentino	Tezze sul Brenta
Molvena	Valstagna

L'organizzazione aziendale è rappresentata dalle tre seguenti articolazioni:

- **Distretto**

cui spetta la gestione caratteristica dell'Azienda. E' la struttura tecnico–funzionale mediante la quale l'Azienda assicura nel proprio ambito territoriale l'erogazione dell'assistenza sanitaria primaria attraverso un elevato livello di integrazione tra i diversi servizi che erogano le prestazioni sanitarie e tra questi i servizi socio – assistenziali in modo da consentire una risposta coordinata e continuativa ai bisogni socio – sanitari della popolazione; esso è centro di riferimento per l'accesso a tutti i servizi dell'Azienda

Sanitaria n. 3, polo unificante di tutti i servizi sanitari, socio-sanitari e socio-assistenziali territoriali, sede di gestione e coordinamento operativo e organizzativo dei servizi territoriali.
L'ambito territoriale dell'Azienda Sanitaria n. 3 è suddiviso nei seguenti distretti socio–sanitari, che garantiscono l'articolazione dell'organizzazione distrettuale in modo equilibratamente diffuso e distribuito sul territorio e che si configurano come strutture complesse:
n. 1 (comprendente 20 Comuni: Bassano del Grappa – Campolongo sul Brenta – Cartigliano – Cassola – Cismon del Grappa – Marostica – Mason Vicentino – Molvena – Mussolente – Nove – Pianezze – Pove del Grappa – Romano d'Ezzelino – Rosà – Rossano Veneto – San Nazario – Schiavon – Solagna – Tezze sul Brenta – Valstagna, con un totale di n. 157.948 abitanti; con sedi operative a Bassano del Grappa, Marostica, San Nazario-Carpanè, Rosà, Rossano Veneto e Tezze sul Brenta; con sede amministrativa direzionale in Bassano del Grappa – via Cereria).
n. 2 (comprendente 8 Comuni: Asiago - Conco – Enego – Foza – Gallio – Lusiana – Roana – Rotzo, con un totale di n. 21.549 abitanti; con sedi operative ad Asiago, Conco, Enego e Lusiana; con sede amministrativa direzionale in Asiago – via Sisemol).

- **Ospedale**

cui spetta la gestione caratteristica dell'Azienda. E' la struttura tecnico-funzionale mediante la quale l'azienda assicura l'assistenza ospedaliera nel proprio bacino territoriale in modo unitario ed integrato sulla base dei principi di programmazione e di organizzazione regionale, perseguendo anche la formazione e la ricerca.
L'Ospedale dell'Azienda U.L.S.S. n. 3 si articola nei due presidi ospedalieri di "S. Bassiano" di Bassano del Grappa e di Asiago, che si configurano come strutture complesse.

- **Dipartimento di Prevenzione**

cui spetta la gestione caratteristica dell'Azienda. E' la struttura tecnico-funzionale mediante la quale l'Azienda assicura nel proprio bacino territoriale la promozione e la tutela della salute della popolazione.
Il Dipartimento di Prevenzione si articola nei seguenti Servizi:

- Servizio Igiene e Sanità Pubblica;
- Servizio Prevenzione, Igiene e Sicurezza degli ambienti di lavoro;
- Servizio Igiene degli Alimenti e della Nutrizione;
- Servizio per l'Educazione e la Promozione della Salute;
- Servizio Sanità Animale;
- Servizio Igiene degli allevamenti e delle produzioni zootecniche;
- Servizio Igiene della produzione, trasformazione, commercializzazione, conservazione e trasporto degli alimenti di origine animale e loro derivati.

5.2 TRATTAMENTI EFFETTUATI DALL'AZIENDA

Con il termine "trattamento", ai sensi dell'art. 4, comma 1, lett. a) del D.lgs. 196/03, 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'AZIENDA SANITARIA ULSS N°3, in quanto organismo sanitario pubblico, tratta dati inerenti la salute.

Qualunque trattamento di dati personali da parte dell'AZIENDA SANITARIA ULSS N°3 è consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18, comma 2 D.lgs. 196/03), 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. 196/03.

Per descrivere sinteticamente i trattamenti effettuati dall'AZIENDA SANITARIA ULSS N°3, i compiti e le relative responsabilità delle singole strutture, in relazione ai trattamenti effettuati, si riporta la seguente tabella.

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Medici e Paramedici di: • Distretti • Ospedali • Dipartimenti Personale di segreteria espressamente autorizzato all'intermediazione tra medico e paziente.	Trattamento di dati di tipo sanitario. Acquisizione, consultazione, registrazione, aggiornamento dati su cartella clinica cartacea/elettronica. Comunicazione dei dati sanitari a soggetti indicati in consenso di Legge.	Trattamento di dati per esecuzione delle obbligazioni di cui al rapporto di cura e assistenza richiesto.
Personale amministrativo di: • Distretti • Ospedali • Dipartimenti Servizi amministrativi. Servizio economico finanziario	Trattamento di dati di tipo contabile e fiscale di fornitori, persone fisiche e giuridiche, pubbliche amministrazioni, enti e associazioni privati che hanno o hanno avuto in qualche modo rapporti anche economici con l'Azienda.	Attività amministrativa connessa all'attività istituzionale.
Servizi Amministrativi; Ufficio qualità e formazione.	Trattamento di dati di tipo contabile e fiscale. Trattamento di dati di dipendenti e professionisti associati.	Acquisizione, organizzazione e gestione delle risorse umane ed informative, finanziarie, patrimoniali e materiali
Servizio per il Sistema Informatico	Trattamento di dati personali di tipo identificativi e sensibili	Predisposizione di misure di sicurezza dei dati trattati e conservati su supporti informatici

	(anche sanitari)	Salvataggio di dati su supporti informatici. Ripristino di dati su supporti informatici.

5.3 SEDI DEL TRATTAMENTO

Il trattamento dei dati è svolto sia nella sede principale dell'AZIENDA SANITARIA ULSS N°3 sia nelle sedi periferiche.
Data la distribuzione geografica, l'elenco delle sedi territoriali in cui avvengono i trattamenti è sintetizzato nell'Atto Aziendale.

5.4 STRUMENTI UTILIZZATI PER IL TRATTAMENTO

Le operazioni di trattamento dei dati indicate dall'art. 4 D.Lgs. n. 196/03 riguardano i trattamenti effettuati con l'ausilio di strumenti elettronici e senza l'ausilio di strumenti elettronici (trattamento su supporto cartaceo).
L'AZIENDA SANITARIA ULSS N°3 effettua trattamenti con e senza l'ausilio di strumenti elettronici.

5.4.1 Documenti cartacei

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

- archivio corrente (insieme dei documenti correnti): tenuto dai singoli Incaricati e Responsabili negli uffici e nelle aree operative, o tenuto dal personale nei reparti di cura;
- archivio storico (insieme dei documenti storici): mantenuto per motivi storici o per esigenze di legge a cura di un incaricato appositamente designato.

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

5.4.2 Strumenti elettronici

Attualmente, presso l'AZIENDA SANITARIA ULSS N°3 la gestione dei dati, vista la particolare articolazione aziendale, non è totalmente centralizzata.

La situazione è schematizzabile nel seguente modo:

GESTIONE DEI DATI	DESCRIZIONE	RESPONSABILITÀ DELLA GESTIONE
GESTIONE LOCALE	Gestioni locali di dati su stazioni di lavoro personali - personal computer/server non connessi in rete o connessi in rete, ma con la possibilità di gestire localmente documenti e/o dati. Presso tutte le sedi dell'AZIENDA SANITARIA ULSS N°3 sono presenti anche applicazioni dedicate, ovvero apparecchiature elettromedicali	Responsabile del centro di responsabilità (o personale delegato a livello di distretto o di reparto) dove sono collocate le stazioni di lavoro o le applicazioni dedicate o le apparecchiature elettromedicali. Il Responsabile del centro di responsabilità, adotta gli atti e le misure necessarie a garantire un adeguato controllo relativamente alle norme di buon uso dei sistemi informatici e di telecomunicazione

	che registrano le informazioni sensibili direttamente in formato elettronico.	dell'azienda nonché le misure di sicurezza contemplate dal Codice (misure di tipo fisico, logico ed organizzativo). Per mettere in atto tali misure può avvalersi anche di strutture esterne.
GESTIONE CENTRALIZZATA	Gestione dei dati residenti sui server presso i locali del Servizio per il Sistema Informatico (nel seguito denominato più semplicemente SSI).	Servizio per il Sistema Informatico. Per la descrizione del sistema informativo e informatico centralizzato si veda l'allegato (v. DPSS-StrumentiElettronici.doc), redatto e aggiornato a cura del personale del Servizio per il Sistema Informatico. Il Servizio per il Sistema Informatico può avvalersi di strutture esterne per la gestione di parco macchine, applicativi e infrastrutture di comunicazione.

Il predetto SSI opera al servizio di tutte le Strutture aziendali dell'AZIENDA SANITARIA ULSS N°3, garantendo la funzionalità e, quindi, la continuità operativa, della rete, delle telecomunicazioni e degli applicativi generali residenti sui server centralizzati.

6. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

6.1 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 della AZIENDA SANITARIA ULSS N°3 è la AZIENDA SANITARIA ULSS N°3.

6.1.1 Compiti del Titolare

Il Titolare provvede nei casi previsti dalla legge:

- ad assolvere l'obbligo di notificazione al Garante;
- a richiedere, ove necessario, le autorizzazioni e ad effettuare le dovute comunicazioni all'Autorità Garante per il trattamento o la comunicazione dei dati;
- ad adottare, per quanto di competenza, le misure necessarie a garantire la sicurezza dei dati personali, redigendo ed aggiornando il Documento Programmatico sulla Sicurezza;
- a nominare uno o più Responsabili anche mediante suddivisione dei compiti;
- ad impartire ai Responsabili le necessarie istruzioni per la corretta gestione e tutela dei dati personali, ivi compresa la salvaguardia della loro integrità e sicurezza;
- a verificare periodicamente l'osservanza dell'attività svolta dai Responsabili rispetto alle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

- a provvedere alla formazione degli incaricati del trattamento dei dati personali, attraverso la previsione di interventi formativi, al fine di 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 medesimo.

Il Titolare del trattamento affida ai Responsabili del trattamento il compito di porre in essere ogni misura tesa a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite con ogni mezzo ritenuto più idoneo.
Il Titolare del trattamento affida ai singoli Responsabili del trattamento l'onere di individuare, nominare ed indicare per iscritto gli Incaricati del trattamento.

6.2 IL RESPONSABILE DEL TRATTAMENTO

Il Responsabile è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposto dal Titolare al Trattamento.

Responsabili del trattamento dei dati personali dell'AZIENDA SANITARIA ULSS N°3 sono i Responsabili dei centri di responsabilità, ciascuno per il proprio livello di responsabilità e per i dati in proprio possesso, nominati con delibera n. 72 del 03.02.2010.

In caso di necessità operative interne alla AZIENDA SANITARIA ULSS N°3 o in caso di assenza o di impedimento, il Responsabile può delegare un proprio rappresentante.

La nomina del Responsabile del trattamento è a tempo indeterminato e decade per revoca o 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.

6.2.1 Compiti del Responsabile

Al Responsabile vengono affidate le incombenze e le responsabilità di cui all'art. 29 del D.lgs. 196/2003, avendo valutato la loro idoneità al rispetto delle caratteristiche di esperienza, capacità ed affidabilità richieste dalla legge per la tutela del trattamento.
Il responsabile ha il potere di compiere tutto quanto sia necessario per il rispetto delle vigenti disposizioni. In particolare, il Responsabile del trattamento dei dati o suo delegato:

- Individua e nomina per iscritto gli Incaricati del trattamento, gli Amministratori di Sistema (per la gestione locale) e i Responsabili esterni del trattamento.
- Provvede, sulla base delle direttive impartite dal Titolare, ad attuare il trattamento o a dare istruzioni per il corretto trattamento dei dati personali eseguendo a tal fine gli opportuni controlli;
- Adotta le misure e dispone gli interventi necessari per la sicurezza della conservazione dei dati e per la correttezza dell'accesso;
- Informa il Titolare nella eventualità che si siano rilevati dei rischi;

Come previsto dal Codice, periodicamente almeno una volta l'anno, il Responsabile effettua la verifica delle condizioni di sussistenza dei profili di autorizzazione degli

Incaricati, degli Amministratori di Sistema locali e dei Responsabili esterni del trattamento che sono stati da lui nominati.

Dovranno essere inviate al Servizio Affari generali e legali:

- copia delle lettere di nomina dei Responsabili estern,
- elenco degli Amministratori di sistema locali,
- copia delle lettere di nomina degli Amministratori di sistema locali.

6.3 GLI INCARICATI DEL TRATTAMENTO

Ai Responsabili del trattamento è affidato il compito di nominare uno o più Incaricati del trattamento dei dati. La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con atto scritto in cui sono specificati i compiti affidati, unitamente ad idonee ed analitiche istruzioni scritte.
Nel designare gli Incaricati del trattamento per iscritto e nell'impartire le istruzioni, il Responsabile, deve prescrivere che gli Incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.
L'aggiornamento ovvero eventuali modifiche che riguardano le nomine degli incaricati oppure il profilo degli incaricati per gli accessi ai sistemi e quindi ai trattamenti, viene puntualmente gestito dal Responsabile diretto.
Esempi di situazioni tipo:

Situazione	Azione	Responsabile
Nuova assunzione	Il responsabile diretto inoltra una richiesta scritta all'Amministratore di sistema affinché generi un profilo utente avente le necessarie autorizzazioni per l'accesso ai sistemi ed alle banche dati. In funzione alle reali necessità operative viene formalizzata una lettera di incarico per l'interessato recante autorizzazioni, banche dati ed ambiti del trattamento per il nuovo assunto	Responsabile diretto
Passaggio ad altro ruolo	Il responsabile diretto inoltra una richiesta scritta all'Amministratore di sistema affinché elimini il profilo esistente e ne generi uno nuovo avente le autorizzazioni necessarie per il nuovo ruolo. Viene rivalutato il profilo e l'incarico e di conseguenza formulata una nuova lettera di incarico corrispondente alle nuove autorizzazioni, banche dati ed ambiti del trattamento per la persona.	Responsabile diretto
Dimissione	Il responsabile diretto inoltra una richiesta scritta all'Amministratore di sistema affinché elimini il profilo esistente.	Responsabile diretto

La nomina degli Incaricati decade per revoca o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

6.3.1 Compiti degli Incaricati

Gli incaricati, nell'espletamento delle proprie funzioni, devono usare la massima riservatezza nella tenuta dei dati e nella conseguente loro protezione, cercando di evitare i

rischi di distruzione o perdita, anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
Per garantire meglio la riservatezza delle informazioni, ad ogni incaricato è stata assegnata una parola chiave ed un codice identificativo personale (credenziali) a suo uso esclusivo e non cedibili a terzi. Ogni incaricato deve inoltre diligentemente custodire i dispositivi in suo possesso e di cui si avvale nell'espletamento delle sue mansioni lavorative.
Nel caso di trattamento di dati personali sensibili o giudiziari, i medesimi devono essere controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e devono essere restituiti al termine delle operazioni affidate.

6.4 AMMINISTRATORI DI SISTEMA

Il Provvedimento del 27 novembre 2008, emesso dal Garante per la protezione dei dati personali, pubblicato sulla Gazzetta Ufficiale n. 300 del 24 dicembre 2008, modificato con Provvedimento del 25 Giugno 2009, prescrive una serie di accorgimenti e misure che tutti i Titolari (o eventualmente i Responsabili) del trattamento di dati personali effettuati con strumenti elettronici devono adottare, relativamente alle attribuzioni delle funzioni di amministratore di sistema.

Fra le attività previste dal suddetto Provvedimento rientrano le seguenti:

- Valutazione delle caratteristiche soggettive;
- Designazioni individuali;
- Elenco degli amministratori di sistema;
- Informativa ai dipendenti sull'elenco degli amministratori di sistema;
- Registrazione degli accessi;
- Verifica dell'operato degli amministratori da parte del Titolare del trattamento.

In applicazione del sopracitato Provvedimento, l'AZIENDA SANITARIA ULSS N°3, come da delibera del Direttore Generale n° 964 del 14/12/2009, provvede pertanto a:

- Identificare gli Amministratori di Sistema previa valutazione delle caratteristiche di esperienza, capacità e affidabilità dei soggetti e in relazione alla mansione da loro svolta; fra questi rientrano tutti coloro i quali risultano essere figure interne o soggetti terzi preposti alla gestione e alla manutenzione di sistemi informativi in senso lato (sistemi, database, apparati di rete/sicurezza e postazioni di lavoro, apparati e procedure di backup, gestione di strumenti e procedure per l'autenticazione e autorizzazione per l'accesso a sistemi e applicazioni) e che potrebbero quindi - in virtù dei particolari privilegi di accesso a sistemi, dati e applicazioni di cui godono - essere tecnicamente in grado di accedere, anche in maniera fortuita, a dati personali.
- Designare gli amministratori di sistema interni mediante apposita lettera di nomina contenente i compiti assegnati e gli ambiti di operatività consentiti. Agli stessi viene richiesto di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
  La nomina ad Amministratore di Sistema è a tempo indeterminato e decade per revoca o dimissioni dello stesso.

- Designare le società e i soggetti terzi che svolgono funzione di amministratore di sistema mediante apposita lettera di nomina recante i compiti assegnati, gli ambiti di operatività consentiti, la richiesta di fornire e mantenere aggiornato l'elenco nominativo degli amministratori di sistema che possono operare su dati personali di cui l'AZIENDA SANITARIA ULSS N°3 è titolare, la richiesta di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
- Predisporre opportuna lettera informativa per il personale dipendente con la quale si comunicano gli estremi identificativi degli Amministratori di Sistema che possono anche indirettamente venire a conoscenza di dati personali di lavoratori dell'AZIENDA SANITARIA ULSS N°3

Ogni variazione degli elenchi degli Amministratori di Sistema (interni e terze parti) viene comunicata al Servizio Affari Generali a cura dei Responsabili del Trattamento per la Gestione Locale e Centralizzata degli strumenti elettronici. Le copie delle lettere e gli elenchi di cui sopra sono custoditi a cura del Servizio Affari Generali.

Il Titolare o il Responsabile da questi designato effettua, almeno una volta l'anno, una verifica sull'operato degli Amministratori di Sistema.

Al fine di consentire al Titolare o al Responsabile da questi designato la verifica dell'operatività degli Amministratori di Sistema, l'AZIENDA SANITARIA ULSS N°3 adotta sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (*access log*) hanno caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e vengono conservate per un periodo non inferiore a sei mesi.

La descrizione tecnica dettagliata della soluzione adottata per la registrazione dei log, redatta a cura del Servizio Sistema Informatico il 04/12/2009, è allegata alla sopracitata delibera del Direttore Generale n° 964 del 14/12/2009,

6.4.1 Compiti degli Amministratori di sistema

Sia per quanto riguarda la Gestione Locale che per quella Centralizzata si vedano al riguardo le lettere di nomina nelle quali è specificato un quadro sintetico delle attività loro affidate.

7. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Data la complessità della struttura e delle svariate tipologie di trattamento e relative finalità, l'AZIENDA SANITARIA ULSS N°3 utilizza numerose banche dati.
Per l'elenco dei trattamenti di dati personali si veda l'allegato DPSS-ElencoTrattamenti.doc, redatto e aggiornato con la collaborazione dei Responsabili del Trattamento o incaricati da essi delegati.
Per l'elenco dei trattamenti, riferiti a dati sensibili e giudiziari, si faccia riferimento a:

- "Regolamento regionale per il trattamento dei dati sensibili e giudiziari" n° 2 del 20/03/2006, emanato dalla Regione Veneto come prescritto dagli artt. 20 e 21 del D. Lgs. 196/2003; detto Regolamento è stato recepito dall'AZIENDA SANITARIA ULSS N°3 con Delibera del Direttore Generale prot. 545 del 11/05/2006.
- "Regolamento regionale n° 1 del 22/03/2007 recante modifiche al Regolamento regionale n° 2/2006 citato al punto precedente; detto Regolamento è stato recepito dall'AZIENDA SANITARIA ULSS N°3 con Delibera del Direttore Generale prot. 618 del 18/07/2007.

I Regolamenti sopracitati sono pubblicati e disponibili per la consultazione sulla rete Intranet dell'Azienda.

8. TRATTAMENTO DEI DATI AFFIDATI ALL'ESTERNO

Il Titolare (e/o il Responsabile interno) del trattamento può affidare il trattamento dei dati in tutto o in parte a soggetti terzi, nominandoli a mezzo lettera di incarico Responsabili Esterni del trattamento.

Il Titolare (e o il Responsabile interno) del trattamento conserva in luogo sicuro le lettere di incarico dei Responsabili Esterni afferenti alla propria area nelle quali è specificato un quadro sintetico delle attività loro affidate, l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, e gli impegni assunti all'esterno per garantire la protezione dei dati stessi.

9. EVENTI E IMPATTI SULLA SICUREZZA

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

		Evento	Descrizione evento	Impatto sulla sicurezza
Eventi relativi al contesto fisico - ambientale	Eventi relativi alle sedi fisiche	Ingressi non autorizzati a locali/aree ad accesso ristretto	Possono verificarsi accessi non autorizzati da parte di persone che si trovano sia all'esterno che all'interno dell'organizzazione.	Accesso a documenti cartacei e strumenti.
		Sottrazione di strumenti contenenti dati	Strumenti contenenti dati (PC, portatili, supporti di memorizzazione,…) possono essere sottratti illecitamente da terzi.	Sottrazione di strumenti contenenti dati. e quindi perdita di dati, in modo illecito.

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

		Rischi connessi a sistemi di climatizzazione	Possono verificarsi malfunzionamenti sui sistemi ausiliari necessari al corretto funzionamento degli apparati HW/SW con i quali viene trattata la banca dati interessata	Perdita parziale o totale dei dati.
		Errori umani nella gestione della sicurezza	A causa di disattenzione possono verificarsi errori nella gestione della sicurezza (lasciare i locali SSI aperti e quindi accessibili a chiunque, mal gestione di strumenti,…).	Perdita, danneggiamento o alterazione di dati importanti.
Eventi relativi agli strumenti	Eventi relativi alle risorse hardware	Uso non autorizzato dell'hardware o di strumenti	Persone non autorizzate possono accedere a risorse hardware o a strumenti danneggiandoli.	Perdita o danneggiamento di hardware o strumenti e quindi di dati.
		Manomissione/sabotaggio degli strumenti	Possono verificarsi malfunzionamenti alle risorse hardware	Perdita di dati, tempi di inattività o perdite di produttività.
		Perdita di dati dovuta ad errori o a guasti	Errori di configurazione dell'hardware o guasti possono provocare malfunzionamenti alle risorse hardware.	Perdita di dati, tempi di inattività o perdite di produttività.
		Rischi connessi all'elettricità	Blackout ripetuti e sbalzi eccessivi delle linee di alimentazione elettrica possono provocare malfunzionamenti alle risorse hardware.	Perdita di dati, tempi di inattività o perdite di produttività.
	Eventi relativi alle risorse	Accesso non autorizzato alle basi dati connesse	Soggetti malintenzionati possono accedere in modo illecito alle banche dati.	Accesso non autorizzato a dati o informazioni importanti o riservate.

		Errori software / errori di configurazione che minacciano l'integrità dei dati	Possono essere presenti nelle applicazioni errori involontari commessi in fase di progettazione e/o implementazione.	Accesso non autorizzato a dati o informazioni importanti o riservate, perdita di dati, manipolazione di dati, distruzione di dati.
		Presenza di codice non conforme alle specifiche del programma	Possono essere presenti applicazioni software "fatte in casa" che non offrono sufficienti garanzie di sicurezza.	Accesso non autorizzato a dati o informazioni importanti o riservate, perdita di dati, manipolazione di dati, distruzione di dati.
		Azione di virus informatici	Utenti interni e/o esterni possono collocare virus, trojan horse o worm e spostarsi all'interno del file system.	Accesso non autorizzato a dati o informazioni importanti o riservate, perdita di dati, manipolazione di dati, distruzione di dati..
	Eventi relativi alle comunicazioni	Accesso non autorizzato alla rete	Soggetti non autorizzati possono accedere alla rete aziendale, agli applicativi e agli strumenti di interoperabilità.	Accesso non autorizzato a dati o informazioni importanti o riservate, perdita di dati, manipolazione di dati, distruzione di dati. Utilizzazione di servizi o risorse di rete.
		Intercettazione di informazioni transitanti sulla rete	Soggetti malintenzionati possono accedere a informazioni transitanti sulla rete.	Accesso non autorizzato a dati o informazioni importanti o riservate.
Eventi relativi al comportamento degli operatori		Accesso non autorizzato ai documenti cartacei	Persone non autorizzate possono accedere a documenti cartacei incustoditi presenti su scrivanie, scaffali a vista, armadi non chiusi, archivi.	Accesso non autorizzato a dati o informazioni importanti o riservate.
		Cancellazione non autorizzata di dati/manomissione di dati	A causa della mancanza di consapevolezza, incuria, distrazione gli utenti possono compiere operazioni errate.	Perdita, danneggiamento o alterazione di dati importanti.

		Sottrazione di credenziali	Password deboli possono essere indovinate da soggetti malintenzionati e utilizzate in modo improprio.	Accesso alle banche dati (e quindi anche a dati particolarmente critici e/o sensibili) protette con tali credenziali.
		Carenza di consapevolezza, disattenzione o incuria	A causa di incuria, disattenzione o scarsa conoscenza degli strumenti gli operatori possono digitare dati errati o compiere operazioni errate.	Perdita, danneggiamento o alterazione di dati importanti.
		Comportamenti sleali o fraudolenti	Gli utenti del trattamento possono compiere operazioni illecite, con comportamento consapevole, sulla banca dati interessata.	Perdita, danneggiamento o alterazione di dati importanti. Sottrazione di dati o informazioni importanti o riservate.

10. MISURE DI SICUREZZA IN ESSERE

Al fine di assicurare

- l'integrità e la disponibilità dei dati,
- la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità,
- il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

ed impedirne la comunicazione e/o diffusione non autorizzata, l'AZIENDA SANITARIA ULSS N°3 ha elaborato una precisa Politica di Sicurezza basata sull'adozione di misure di tipo fisico, logico ed organizzativo. Tali misure avranno il compito di garantire sia i minimi requisiti di sicurezza contemplati dal Codice, sia un livello idoneo di sicurezza relativamente alle tipologie dei dati trattati, alle modalità di trattamento ed agli strumenti utilizzati.

Locali SSI

Cod.	Evento	Misure adottate	Trattamenti interessati
C01	Ingressi non autorizzati a locali/aree ad accesso ristretto Sottrazione di strumenti contenenti dati	I locali SSI hanno un'unica porta di accesso comandata da un sistema di controllo accessi che utilizza un badge magnetico. In tal modo tutti gli accessi vengono registrati. Solo il personale SSI entra utilizzando il badge. La sala server, interna all'area uffici SSI, è protetta da una porta che è possibile chiudere	Trattamenti informatici

Cod.	Evento	Misure adottate	Trattamenti interessati
		a chiave ed è protetta da allarme acustico.	
C02	Ingressi non autorizzati a locali/aree ad accesso ristretto Sottrazione di strumenti contenenti dati	L'accesso ai locali nei quali sono ospitati i sistemi di elaborazione o i sistemi di comunicazione è interdetto a chiunque, fatta eccezione per il personale autorizzato. Se eventualmente si rendesse necessario l'accesso a detti locali da parte di personale non autorizzato - per es. da parte di tecnici della manutenzione di ditte fornitrici, ecc., i visitatori vengono opportunamente identificati a vista a mezzo videocitofono e accompagnati durante tutta la loro permanenza in detti locali da personale autorizzato. Deroghe a tale regola potranno essere concesse solo dietro precisa motivazione e andranno comunque segnalate all'Amministratore di Sistema. I locali dove sono ospitati i sistemi di elaborazione e i sistemi di comunicazione più critici sono videosorvegliati garantendo la registrazione dei movimenti delle persone. I cavi di collegamento alla rete sono organizzati in armadi, dotati di chiusura a chiave ed appositamente etichettati. I collegamenti fisici effettuati solo dal personale autorizzato, sono riportati e siglati in un registro appositamente predisposto a livello di armadio e contenuto all'interno dell'armadio medesimo.	Trattamenti informatici
C03	Calamità naturali	Tutti i pavimenti dei locali SSI sono sopraelevati. E' presente un impianto antincendio nei locali SSI. I dati personali vengono salvati con frequenza giornaliera e per gli applicativi particolarmente critici con frequenza plurigiornaliera.	Tutti i trattamenti
C04	Rischi connessi a sistemi di climatizzazione	La sala server è dotata di impianto di climatizzazione opportunamente dimensionato.	Trattamenti di tipo informatico
C05	Rischi connessi	I server sono assistiti da un sistema UPS che garantisce circa 2 ore di funzionamento. I	Trattamenti di tipo

Cod.	Evento	Misure adottate	Trattamenti interessati
	all'elettricità	server sono dotati di un doppio alimentatore ognuno dei quali è assistito da un UPS diverso e sono posti sotto un gruppo di continuità elettrogeno. Gli apparati di rete più critici sono assistiti, oltre che dal sistema UPS dell'Ospedale, anche da un sistema UPS dedicato.	informatico
C06	Manomissione/sabotaggio degli strumenti	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia. I manutentori esterni firmano un modulo di intervento, gestito in forma mista cartacea e informatica, che verrà integrato con una dichiarazione di conformità al D. Lgs. 196/2003.	Trattamenti di tipo informatico
C07	Perdita di dati dovuta ad errori o a guasti	L'hardware che si utilizza è di qualità e storicamente non ha mai dato problemi rilevanti. Tutti i server hanno: Sistema Raid – Doppia Alimentazione – Cluster Le attrezzature sono buona qualità e coperte da garanzia	Trattamenti di tipo informatico
C08	Perdita di dati dovuta ad errori o a guasti Errori umani	I dati personali gestiti centralmente vengono salvati con frequenza plurigiornaliera, giornaliera, settimanale, secondo una metodica che consente di disporre in ogni momento delle copie di salvataggio. I server hanno dischi mirrorati in alta affidabilità (tipo RAID1, RAID5 e RAID DP).	Trattamenti di tipo informatico

Altri locali

Cod.	Evento	Misure adottate	Trattamenti interessati	Struttura o persone addette all'adozione
M01	Ingressi non autorizzati a locali/aree ad accesso ristretto	E' presente un servizio di vigilanza comprendente pattugliamenti giornalieri.	Tutti i trattamenti	Ospedale San Bassiano di Bassano del Grappa

Cod.	Evento	Misure adottate	Trattamenti interessati	Struttura o persone addette all'adozione
	Sottrazione di strumenti contenenti dati Sottrazione di documenti cartacei Manomissione /sabotaggio degli strumenti Accesso non autorizzato ai documenti cartacei	E' presente un servizio di vigilanza comprendente il pattugliamento notturno con 3 ispezioni.	Tutti i trattamenti	Centro Socio Sanitario Mons. Egidio Negrin di Bassano del Grappa / Palazzine B, D, F, G.
		E' presente un servizio di vigilanza comprendente il pattugliamento notturno con 3 ispezioni.	Tutti i trattamenti	Sede C.E.O.D. di Bassano del Grappa / Fabbricato principale
		E' presente un servizio di vigilanza comprendente il pattugliamento notturno con 3 ispezioni.	Tutti i trattamenti	Centro Socio Sanitario Prospero Alpino di Marostica / Palazzina ospitante gli uffici amministrativi del Distretto ed il Servizio Veterinario
		I locali sono costantemente presidiati dal personale durante il giorno. Allo scadere dell'orario di sportello, le porte di accesso vengono chiuse e nessun utente dei servizi è ammesso, se non personalmente accompagnato da personale autorizzato. Il personale dipendente ogni giorno timbra l'entrata/uscita per l'accesso agli uffici; per gli utenti ed i visitatori non esiste una registrazione ad eccezione degli uffici che	Tutti i trattamenti	Altre sedi

Cod.	Evento	Misure adottate	Trattamenti interessati	Struttura o persone addette all'adozione
		erogano servizi al pubblico e del Pronto Soccorso, le cui modalità sono diversificate in funzione dei servizi erogati agli utenti che usufruiscono delle prestazioni.		
		Sono presenti impianti di videosorveglianza atti a monitorare le aree del P.O. San Bassiano.	Tutti i trattamenti	P.O. San Bassiano/ex struttura ospedaliera di Mezz.va
M02	Sottrazione di strumenti contenenti dati Sottrazione di documenti cartacei Manomissione /sabotaggio degli strumenti Ingressi non autorizzati a locali/aree ad accesso ristretto	I flussi relativi a personale NON dipendente sono identificabili in due tipologie: gli assistiti ed eventuali parenti o affini ed i terzi prestatori d'opera (dipendenti di imprese esterne, consulenti, ecc). In entrambi i casi il personale consente loro l'accesso ai locali filtrandoli al momento del loro ingresso. Gli addetti sono tenuti ad effettuare vigilanza contro il rischio di accesso di persone non autorizzate.	Tutti i trattamenti	Tutte le sedi
M03	Calamità naturali	Non tutti gli elaboratori sono sollevati da terra. 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.	Tutti i trattamenti	Tutte le sedi
M04	Uso non autorizzato dell'hardware	Tutti gli accessi ai personal computer non collegati a strumenti elettromedicali sono gestiti mediante account centralizzati di active directory.	Trattamenti di tipo informatico	Tutte le sedi

Cod.	Evento	Misure adottate	Trattamenti interessati	Struttura o persone addette all'adozione
	Accesso non autorizzato alle basi dati connesse Cancellazione non autorizzata di dati/manomissione di dati Sottrazione di credenziali di autenticazione Accesso non autorizzato alla rete	Agli incaricati sono state assegnate le credenziali di autenticazione consistenti in un codice per l'identificazione, che neppure in futuro potrà essere associato ad altre persone, unito a una parola chiave riservata conosciuta solamente dall'incaricato. La parola chiave è composta da otto caratteri; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata ogni 90 giorni. Per agevolare e garantire l'applicazione di questa misura di sicurezza è già stato adottato per buona parte degli utenti un meccanismo di scadenza automatica delle password ogni 90 giorni, che verrà esteso a tutti gli incaricati dell'Azienda Sanitaria entro il corrente anno. 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.	Trattamenti di tipo informatico	Gestione centralizzata
M05	Accesso non autorizzato alle basi dati connesse Intercettazione di informazioni	Tutti gli accessi a Internet, gestiti in modo centralizzato, avvengono tramite un Server ISA che funge da Proxy e da Firewall.	Trattamenti di tipo informatico	Gestione centralizzata

Cod.	Evento	Misure adottate	Trattamenti interessati	Struttura o persone addette all'adozione
	transitanti sulla rete			
M06	Manomissione /sabotaggio degli strumenti	Alle risorse non accedono persone non autorizzate. La manutenzione è effettuata da tecnici di fiducia.	Trattamenti di tipo informatico	Gestione centralizzata
M07	Perdita di dati dovuta ad errori o a guasti	L'hardware che si utilizza è di qualità e storicamente non ha mai dato problemi rilevanti. Le attrezzature sono buona qualità e coperte da garanzia	Trattamenti di tipo informatico	Gestione centralizzata
M08	Errori software che minacciano l'integrità dei dati	Gli aggiornamenti dei programmi per elaboratore sono effettuati periodicamente.	Trattamenti di tipo informatico	Gestione centralizzata
M09	Perdita di dati dovuta ad errori o a guasti Errori umani	I dati personali vengono salvati con frequenza plurigiornaliera, giornaliera, settimanale, secondo una metodica che consente di disporre in ogni momento delle copie di salvataggio.	Trattamenti di tipo informatico	Gestione centralizzata
		Salvataggio a cura del Responsabile del centro di responsabilità (o personale delegato a livello di distretto o di reparto).	Trattamenti di tipo informatico	Gestione locale
M10	Azione di virus informatici Presenza di codice non conforme alle specifiche del programma	La protezione di tutti i posti di lavoro collegati alla rete, dei server e delle postazioni mobili viene assicurata attraverso un antivirus server che garantisce l'aggiornamento automatico del Data Base dei virus attraverso un collegamento al sito McAfee che viene attivato con frequenza giornaliera. La scansione sui posti di lavoro viene effettuata con frequenza giornaliera.	Trattamenti di tipo informatico	Gestione centralizzata
M11	Accesso non	**Documenti cartacei:** Quando gli atti e i	Trattamen	Tutte le

Cod.	Evento	Misure adottate	Trattamenti interessati	Struttura o persone addette all'adozione
	autorizzato ai documenti cartacei Sottrazione di documenti cartacei	documenti contenenti dati personali sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione. Gli atti e i documenti vengono restituiti al termine delle operazioni affidate, ovvero ricollocati nel posto in cui sono stati prelevati (ad es. archivio o schedario delle pratiche in corso). Ai Responsabili ed Incaricati sono state impartite istruzioni affinché atti e documenti cartacei (anche lettere o comunicazioni pervenute tramite la posta o a mezzo telefax) od i fascicoli di pratiche non vengano lasciati sparsi sulle scrivanie o appoggiati su ripiani o in luoghi in cui siano visibili a terzi non autorizzati, che possono venirne a conoscenza e divulgarli. Eventuali fotocopie o copie di documenti devono essere custodite con le stesse modalità dei documenti originali. La distruzione definitiva dei documenti cartacei deve avvenire in modo controllato ed in modalità tale da assicurare il non riutilizzo dei dati. L'ubicazione di stampanti ed apparecchi telefax tradizionali non consente ad esterni di leggere od asportare eventualmente documenti non ancora prelevati dal personale. **Archivio corrente**: Tutti i documenti cartacei contenenti dati personali (ivi compresi i dati sensibili e giudiziari) sono conservati in armadi dotati di serratura. Le aree contenenti dati cartacei sono ubicate in modo tale che ciascun addetto	ti di tipo cartaceo	sedi

Cod.	Evento	Misure adottate	Trattamenti interessati	Struttura o persone addette all'adozione
		possa rilevare a vista il tentativo di accesso da parte di persone non autorizzate e, di conseguenza, impedirne l'accesso stesso. Nel corso del trattamento i documenti sono custoditi dal personale incaricato. **Archivio storico**: L'accesso agli archivi storici è consentito esclusivamente agli Incaricati autorizzati.		
M12	Carenza di consapevolezza, disattenzione o incuria Comportamenti sleali o fraudolenti Sottrazione di credenziali di autenticazione	Sono previsti incontri formativi di sensibilizzazione, informazione e aggiornamento agli incaricati sulla corretta modalità operativa per il trattamento dei dati e sui nuovi strumenti e /o misure di sicurezza implementati in azienda.	Tutti i trattamenti	Tutte le sedi

11. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

Il D. lgs. 196/2003 ha per finalità quella di garantire che "il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

Sulla base di quanto prescritto da tale Codice, vengono individuati tre requisiti di sicurezza, che costituiscono il riferimento per valutare il proprio grado di corrispondenza rispetto a quanto indicato dal D. lgs. 196/2003.

I tre requisiti sono:

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

- raccolta,
- registrazione,

- organizzazione,
- conservazione,
- comunicazione,
- diffusione,
- selezione,
- estrazione,
- raffronto,
- interconnessione,
- utilizzo

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

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

disponibilità: tale requisito si riferisce alla necessità di intraprendere azioni in grado di proteggere dati personale, sensibili e giudiziari da possibili eventi che possono ridurre la capacità dell'azienda di assolvere alle finalità di trattamento per cui tali dati sono stati raccolti.

Tali requisiti forniscono quindi un punto di partenza per l'identificazione dei possibili attacchi, individuabili in base all'analisi dello scenario effettuata, e servono alla definizione dei criteri di protezione più adeguati a garantire tale necessità di protezione.

In questa sezione viene data una valutazione qualitativa dei rischi. Al risultato si è arrivati grazie alla combinazione di questionari e interviste aperte che hanno coinvolto gruppi diversificati di persone che operano all'interno dell'AZIENDA SANITARIA ULSS N°3.

Il **rischio da abbattere** è la probabilità che si verifichi un impatto sulle attività aziendali.

Probabilità evento	Descrizione
0	Poco probabile
1	Probabile
2	Verosimile

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

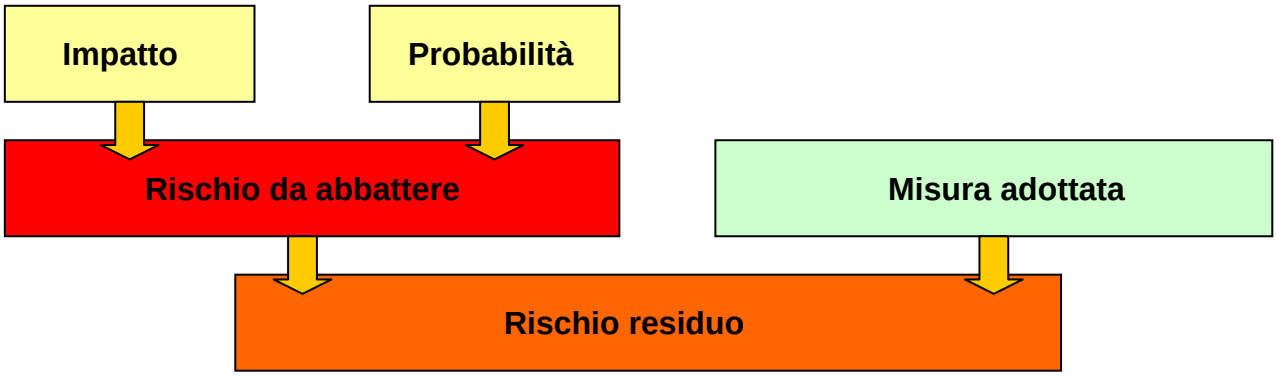
RISCHIO DA ABBATTERE

IMPATTO			
2	0	2	4
1	0	1	2

0	0	0	0
	0	1	2

PROBABILITÀ

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



Il **rischio residuo** è:

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

L'esistenza di un **rischio residuo** (indipendentemente che sia basso, medio o alto) significa prendere atto che la sicurezza assoluta non è un obiettivo conseguibile.

Pertanto è necessario prevedere, accanto alle misure adottate, anche le modalità di gestione dell'evento e quella delle situazioni post evento, nelle quali deve trovare spazio la convivenza con una quota non eliminabile di **rischio residuo**.

Nella tabella seguente viene calcolato il rischio residuo dell'AZIENDA SANITARIA ULSS N°3.

		Evento	Impatto (0-2)	Prob. (0-2)	Rischio da abbattere IxP (0-4)	Misure adottate	Rischio residuo

		Evento	Impatto (0-2)	Prob. (0-2)	Rischio da abbattere IxP (0-4)	Misure adottate	Rischio residuo
ANALISI DEI RISCHI RELATIVI AL CONTESTO FISICO-AMBIENTALE	Analisi dei rischi sulle sedi fisiche	Ingressi non autorizzati a locali/aree ad accesso ristretto	2	1	2	M01 M02	
		Sottrazione di strumenti contenenti dati	2	0	0	M01 M02	
		Sottrazione di credenziali di autenticazione	2	1	2	M04 M12	
		Sottrazione di documenti cartacei	2	1	2	M01 M02 M11	
		Calamità naturali	2	0	0	M03	
		Errori umani	1	1	1	M09	
	Analisi dei rischi nei locali SSI	Ingressi non autorizzati a locali/aree ad accesso ristretto	1	1	1	C01 C02	
		Sottrazione di strumenti contenenti dati	2	0	0	C01 C02	
		Calamità naturali	2	0	0	C03	
		Rischi connessi a sistemi di climatizzazione	1	1	1	C04	
		Rischi connessi all'elettricità	2	2	4	C05	
		Manomissione/sabotaggio degli strumenti	2	1	2	C06	

		Evento	Impatto (0-2)	Prob. (0-2)	Rischio da abbattere IxP (0-4)	Misure adottate	Rischio residuo
		Perdita di dati dovuta ad errori o a guasti	2	2	4	C07 C08	
		Errori umani nella gestione della sicurezza	1	1	1	C08	
ANALISI DEI RISCHI RELATIVI AGLI STRUMENTI	Analisi dei rischi sulle risorse hardware	Uso non autorizzato dell'hardware o di strumenti	1	1	1	M04	
		Manomissione/sabotaggio degli strumenti	2	1	2	M01 M02 M06	
		Perdita di dati dovuta ad errori o a guasti	2	2	4	M07 M09	
	Analisi dei rischi sulle risorse software	Accesso non autorizzato alle basi dati connesse	2	2	4	M04 M05	
		Errori software / errori di configurazione che minacciano l'integrità dei dati	2	2	4	M08	
		Presenza di codice non conforme alle specifiche del programma	2	2	4	M10	
		Azione di virus informatici	2	2	4	M10	

		Evento	Impatto (0-2)	Prob. (0-2)	Rischio da abbattere IxP (0-4)	Misure adottate	Rischio residuo
	Analisi dei rischi sulle comunicazioni	Accesso non autorizzato alla rete	2	2	4	M04	
		Intercettazione di informazioni transitanti sulla rete	2	2	4	M05	
ANALISI DEI RISCHI RELATIVI AI COMPORTAMENTI DEGLI OPERATORI		Accesso non autorizzato ai documenti cartacei	2	2	4	M01 M11	
		Cancellazione non autorizzata di dati/manomissione di dati	2	1	2	M04	
		Sottrazione di credenziali	2	1	2	M04 M12	
		Carenza di consapevolezza, disattenzione o incuria	2	1	2	M12	
		Comportamenti sleali o fraudolenti	2	0	0	M12	

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

12.1 GESTIONE CENTRALIZZATA

Si veda l'allegato DPSS-StrumentiElettronici.doc

12.2 GESTIONE LOCALE

12.2.1 Procedure per il salvataggio regolare dei dati

Il salvataggio dei dati è una procedura che ricopre una funzione cruciale. Attraverso questa procedura, è possibile, in caso di guasto hardware dei dischi, "ripristinare" il sistema nello stesso stato in cui si trovava nel momento dell'ultimo salvataggio.
Viene effettuato salvataggio periodico a carico del Responsabile del centro di responsabilità (o personale delegato a livello di distretto o di reparto).

12.2.2 Procedure per l'archiviazione dei supporti di memorizzazione

I supporti di memorizzazione vengono etichettati con informazione per l'identificazione e conservati.

12.2.3 Procedure per la verifica della leggibilità dei supporti di memorizzazione

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

12.2.4 Criteri per l'eliminazione dei supporti di memorizzazione obsoleti

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

I supporti di memorizzazione possono essere riutilizzati da altri incaricati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

12.2.5 Misure per la custodia dei supporti di memorizzazione

I supporti di memorizzazione utilizzati per l'attività di salvataggio sono conservati in luogo sicuro.

12.2.6 Prove di ripristino

Periodicamente vengono eseguite prove di ripristino dei dati dall'Incaricato delle copie di sicurezza.

12.2.7 Piano di continuità operativa

L'obiettivo del piano di continuità operativa è quello di garantire la continuità del servizio informatico e la disponibilità delle informazioni, evitando o limitando i danni al patrimonio informativo a fronte di un'emergenza.
Il piano di continuità operativa non deve essere inteso come misura alternativa a quelle di prevenzione, ma a completamento di queste ultime.
Allo scopo di gestire gli eventi critici e i disastri quali cessazione temporanea della corrente elettrica, presenza di Virus informatici provenienti da fonti esterne (Internet, floppy ecc…) per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, l'AZIENDA SANITARIA ULSS N°3 ha adottato le seguenti misure:

- salvataggio dei dati
- etichettatura dei supporti di memorizzazione con informazione per l'identificazione
- verifica dell'integrità dell'informazione memorizzata

- custodia dei supporti in luogo sicuro
- eliminazione dei supporti di memorizzazione e dell'informazione in essi contenuta

13. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

L''AZIENDA SANITARIA ULSS N°3 ha effettuato incontri formativi di sensibilizzazione, informazione e aggiornamento per i responsabili e gli incaricati sulla corretta modalità operativa per il trattamento dei dati e sui nuovi strumenti e/o misure di sicurezza implementati in azienda.

Descrizione sintetica degli incontri formativi	Classi di incarico o tipologie di personale interessato
• Panoramica sugli adempimenti del CODICE • Analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, interessato • Misure minime ed appropriate di sicurezza con particolare riferimento a: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software (in particolare antivirus e misure antihacker), contenitori di sicurezza, sistemi anti intrusione, importanza e modalità di realizzazione delle operazioni di backup, utilizzo di internet e posta elettronica etc..	Tutti gli incaricati
• Analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee • Adempimenti del CODICE	Tutti i Responsabili

Coerentemente con l'evoluzione degli strumenti tecnici adottati dalla AZIENDA SANITARIA ULSS N°3 e/o all'insorgere di nuove disposizioni legislative in materia, nonché al momento dell'ingresso in servizio o occasione di cambiamenti di mansioni, verranno istituiti nuovi incontri formativi a cura di ciascun Responsabile del Trattamento. In particolare nel corso del 2010 verranno effettuati incontri formativi teorico pratici direttamente presso le Unità Operative con lo scopo di verificare lo stato di attuazione della normativa nella pratica quotidiana, identificare le aree di miglioramento, aumentare il livello di consapevolezza degli incaricati e dei responsabili

14. CRITERI PER LA CIFRATURA O PER LA SEPARAZIONE DI DATI

La AZIENDA SANITARIA ULSS N°3, essendo un'azienda pubblica che eroga servizi sanitari, ha adottato criteri per la cifratura o per la separazione dei dati come richiesto dal CODICE.
Nella tabella successiva vengono descritte le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura (o la separazione fra dati identificativi e dati sensibili), nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti.

Trattamenti di dati	Protezione scelta (Cifratura/Separazione)	Tecnica adottata	
		Descrizione	Informazioni utili
Sanitari contenuti in "cartella clinica" cartacea	Separazione	Sull'esterno della cartella non è indicato il nominativo del paziente ma codice identificativo	L'attribuzione del codice al paziente avviene attraverso tabella riepilogativa dei pazienti e dei

		composto da numero progressivo e anno in cui il paziente è stato visitato per la prima volta.	relativi codici presente su supporto informatico in dotazione al personale medico, paramedico e di segreteria che fa da intermediazione tra medico e paziente.
Sanitari campioni di materiali biologici / istologici	Separazione	Sul contenitore del campione biologico/istologico non è indicato il nominativo del paziente ma codice identificativo composto da numero progressivo e anno in cui il paziente è stato visitato per la prima volta.	L'attribuzione del codice al paziente avviene attraverso tabella riepilogativa dei pazienti e dei relativi codici presente su supporto informatico in dotazione al personale medico, paramedico e di segreteria che fa da intermediazione tra medico e paziente.

Per quanto riguarda i dati trattati mediante strumenti informatici la gestione viene effettuata attraverso l'impiego di Data Base di tipo relazionale. Questi ultimi consentono la separazione del dato sanitario dagli altri dati personali degli interessati; ciò è reso possibile mediante l'archiviazione dei dati sanitari e di quelli identificativi in tabelle separate, in modo da non permettere l'immediata riconducibilità del dato sanitario al paziente al quale tale dato è riferito. Gli operatori dell'Azienda Sanitaria sono messi in grado di accedere esclusivamente ai dati di propria competenza attraverso meccanismi di profilazione degli utenti resi possibili dalle applicazioni software. Per ogni singolo utente la profilazione viene impostata e mantenuta aggiornata sulla base degli ambiti di trattamento consentiti, con la collaborazione degli amministratori dei sistemi centralizzati e locali.

15. MISURE DI SICUREZZA DA ADOTTARE

Misure da adottate	Obiettivo - Rischi da contrastare	Trattamenti interessati	Struttura o persone addette all'adozione	Tempi previsti per la messa in opera
Adozione di un sistema di protezione preventiva e	Riduzione e-mail di spam.	Tutti i trattamenti	Tutte le sedi	30/06/2010

controllo dello spam in aggiunta ai normali criteri di protezione presenti nel server Exchange.		informatici		
Adozione di un sistema di web filtering	Prevenzione del traffico internet verso siti non autorizzati	Tutti i trattamenti informatici	Tutte le sedi	31/12/2010
Completamento della impostazione -per tutti gli utenti di strumenti informatici- del meccanismo di scadenza automatica delle password ogni 90 giorni	Garantire in maniera certa l'applicazione corretta del cambio password da parte di tutti gli incaricati	Tutti i trattamenti informatici	Sistemi con gestione centralizzata	31/12/2010

16. PERIODICITÀ DI REVISIONE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

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

17. ALLEGATI

Riferimento paragrafo	Codice documento	Descrizione
5.4.2 12.1	DPSS-StrumentiElettronici.doc	Descrizione del sistema informativo e informatico centralizzato
7	DPSS-ElencoTrattamenti.doc	Elenco dei trattamenti effettuati dall'Azienda