DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi del D.Lgs. 196/2003

con riferimento alle Misure di Sicurezza di cui dagli artt. dal 31 al 36

ed al Disciplinare Tecnico di cui all'Allegato B al Codice

CASA DI RIPOSO

DI BRICHERASIO

INDICE

1. **PREMESSE**
2. **ANALISI DEI RISCHI**
3. **ELENCO DEI TRATTAMENTI**
4. **DISTRIBUZIONE DEI COMPITI**
5. **DISPOSIZIONI SULL'ACCESSO AI LOCALI ED AI DATI PERSONALI**
    a. **MISURE DI SICUREZZA FISICHE**
    b. **MISURE DI SICUREZZA INFORMATICHE**
6. **PREVISIONE DI INTERVENTI FORMATIVI**

CONCLUSIONI ED ISTRUZIONI PER L'AGGIORNAMENTO DEL DPS

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

ai sensi del D.Lgs. 196/2003

Ai sensi degli artt. dal 31 al 36 del Decreto Legislativo 196 del 30 giugno 2003 (d'ora in avanti indicato come "Testo Unico"), ed in relazione a quanto previsto dall'Allegato B al predetto decreto, la Casa di Riposo di Bricherasio adotta il seguente Documento Programmatico sulla Sicurezza (d'ora in avanti indicato più sinteticamente come "DPS").

1. PREMESSE

Premesso che:

- La Casa di Riposo di Bricherasio effettua, ai sensi del Testo Unico sulla Privacy, trattamenti di dati personali;
- La Casa di Riposo di Bricherasio, ai sensi della medesima norma è da considerare "titolare" del trattamento dei dati personali;
- Il trattamento dei dati è effettuato tanto attraverso l'utilizzo di documenti cartacei, quanto con il ricorso ad elaboratori elettronici;
- Il trattamento dei dati interessa sia dati genericamente "personali", sia dati personali "sensibili", così come definiti rispettivamente dall'art. 4, comma 1, lett. b) e d) del Testo Unico.

Si stabilisce che:

Il trattamento dei dati personali, specialmente per quanto concerne l'adozione delle misure minime di sicurezza - così come regolamentate dall'art. 31 e dall'Allegato B del Testo Unico – e di altre eventuali misure di sicurezza, sia svolto in conformità alle indicazioni contenute nel DPS, il quale è stato steso al fine di:

- conferire dignità documentale al processo di adeguamento alla normativa sulla riservatezza dei dati personali, svolto nei termini previsti dalla stessa;

- descrivere lo stato delle cose alla data odierna, cui si riferisce la presente verbalizzazione, con la precisazione che il documento rappresenta un'attestazione di quanto esisteva già in passato e di cui ora si prende formalmente atto.

2. ANALISI DEI RISCHI

La valutazione dei rischi cui sono esposti i dati trattati dalla Casa di Riposo di Bricherasio è stata effettuata tenendo presente che:

- i locali della Casa di Riposo di Bricherasio sono situati tutti presso la sede di Via Bell Ville 12;

  la palazzina è di due piani di cui uno è il piano terreno; l'entrata è cintata e controllata con all'interno un giardino.

  La struttura è autorizzata per un totale di 36 posti letto, divisi in reparto RSA (Residenza Sanitaria Assistita) e RAA (Residenza Alberghiera Assistenziale) su entrambi i piani.

  L'ufficio amministrativo è situato al piano terra, così come altri locali come lo spogliatoio del personale, mentre al primo piano vi è l'infermeria ove sono conservate le cartelle cliniche ed altri dati sanitari degli ospiti, oltre alla cucinetta dove è gestito il quaderno delle consegne. Il resto delle struttura, oltre naturalmente alle camere, è composto dalla cucina, dalla sala refettorio, la palestra, la lavanderia e da altri locali.

  L'archivio storico e corrente è conservato al piano terreno in locali chiusi a chiave.

  In tutti questi locali sono effettuati trattamenti rilevanti ai fini dell'applicazione del DPS, anche di dati sensibili in particolar modo sanitari, per cui i luoghi di lavoro devono sottostare alle più restrittive e rigorose norme sulla protezione di simili dati.

- in tutti i locali menzionati sono conservati e trattati informazioni personali in forma cartacea. Nell'Ufficio amministrativo vi sono due Personal computer su cui vengono effettuati trattamenti di dati personali, in infermeria vi sono due PC (uno collegato in rete con gli uffici amministrativi e l'altro no) che vengono utilizzati dal personale sanitario, dalla fisioterapista, dall'animatrice, dalla referente CM Service.

- l'edificio è provvisto di un impianto di allarme relativo ad evitare intrusioni di soggetti dall'esterno;

- Per quanto riguarda la struttura fisica degli Uffici, della Cucina, dei Reparti e dell'Infermeria,

possiamo sintetizzare che:

ogni locale è dotato di una o più porte d'accesso munite di serratura, nonché di finestre con maniglie,

porte e finestre sono in buono stato di manutenzione e conservazione,

ogni locale ha a disposizione armadi e cassetti dotati di serratura.

Le camere relative agli ospiti, ove esiste trattamento di dati personali, sono dotate di armadi e di cassettiere personali dotate di serratura.

In considerazione di tali elementi, si è pervenuti alla conclusione che:

- i dati trattati dalla Casa di Riposo di Bricherasio sono esposti agli ordinari rischi propri di qualsiasi sito fisicamente accessibile, oltretutto attenuati dalla congruità della dotazione strutturale e dall'assenza, in passato, di significative infrazioni negli edifici ove vengono effettuati i trattamenti;
- dipendenti, collaboratori ed ogni altro soggetto Incaricato, non costituiscono, con il proprio comportamento che si deve conformare alle prescrizioni ed indicazioni ricevute, un rilevante fattore di rischio per i dati trattati, ma – poiché le mansioni risultano particolarmente flessibili e vaste – essi devono essere adeguatamente responsabilizzati e controllati;
- le postazioni di lavoro meccanizzate non costituiscono un particolare fattore di criticità, poiché beneficiano – in termini di sicurezza fisica – dell'adeguatezza della struttura complessiva e – in termini di sicurezza logica – sono gestite da soggetti che devono seguire precise indicazioni e prescrizioni volte a ridurre al minimo ogni possibile danno proveniente dall'esterno (virus, sabotaggi, ecc. anche proveniente dal collegamento ad Internet).

Riportiamo una Tabella di Analisi e di riassunto dei principali rischi, dal punto di vista dell'applicazione della normativa sulla Privacy, a cui la Ns. struttura potrebbe potenzialmente andare incontro.

Tabella di Analisi dei rischi

Rischi		Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)
Comportamenti degli operatori	sottrazione di credenziali di autenticazione	Bassa per Ufficio Amministrativo Alta per eventuale PC infermerie
	carenza di consapevolezza, disattenzione o incuria	Media
	comportamenti sleali o fraudolenti	Alta
	errore materiale	Alta in relazione al trattamento di dati sanitari Bassa negli altri casi
	altro evento	Alta in relazione al trattamento di dati sanitari Bassa negli altri casi
Eventi relativi agli strumenti	azione di *virus* informatici o di programmi suscettibili di recare danno	Bassa (esiste documentazione cartacea di riferimento)
	spamming o tecniche di sabotaggio	Bassa
	malfunzionamento, indisponibilità o degrado degli strumenti	Bassa (esiste documentazione cartacea di riferimento)
	accessi esterni non autorizzati	Media
	intercettazione di informazioni in rete	Alta (ove esistano collegamenti in rete)
	altro evento	Bassa (esiste documentazione cartacea di riferimento)
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	Media in generale Alta se accesso nelle infermerie
	sottrazione di strumenti contenenti dati	Alta se contengono dati sanitari Bassa negli altri casi
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.) nonché dolosi, accidentali o dovuti ad incuria	Alta con riferimento ai dati sanitari Bassa negli altri casi
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)	Bassa
	errori umani nella gestione della sicurezza fisica	Alta con riferimento alle infermerie Bassa negli altri casi
	altro evento	Alta con riferimento ai dati sanitari Bassa negli altri casi

3. ELENCO DEI TRATTAMENTI

I trattamenti dei dati personali posti in essere dalla Casa di Riposo di Bricherasio in relazione a quanto definito dal Testo Unico, sono svolti in relazione alle finalità assistenziali e previdenziali della struttura, e pur partendo da una base dati comune, vengono svolti attraverso l'utilizzo di diverse banche dati. Allo stato attuale i trattamenti effettuati dalla struttura, possono essere classificati con il seguente schema, che introduce sia una divisione relativa alla natura dei dati trattati (C-Comuni, S- sensibili), sia in relazione agli strumenti di trattamento utilizzati (C-carta, I-informatici). In quest'ultimo caso verrà segnalata la prevalenza del trattamento, considerando quindi quali siano le Banche Dati prevalentemente utilizzate a tal fine (cioè se sono prevalenti i dati provenienti da strumenti informatici o viceversa da documenti cartacei).

Tabella 1.1: Elenco dei trattamenti

Identificativo del Trattamento	Descrizione sintetica	Natura dei dati trattati		Struttura di riferimento	Altre strutture esterne che concorrono al trattamento	Descrizione degli strumenti utilizzati (Banca dati prevalente)
1.a	Contabilità	C		Ufficio Amministrativo	ENTI REV CBA INFORMATICA SRL UNICREDIT S.P.A.	I
2.a	Delibere e determine	C	S	Ufficio Amministrativo	Dott.ssa Genta Daniela	C
3.a	Aspiranti Ospiti	C	S	Ufficio Amministrativo	Medici di base Direttore Sanitario	C
4.a	Ospiti per finalità amministrative	C		Ufficio Amministrativo	Dott.ssa Genta Daniela CBA INFORMATICA	I
5.a	Corrispondenza ed altri documenti	C		Ufficio Amministrativo	NO	C
6.i	Dati sanitari ospiti (anche cartelle cliniche)	C	S	Esterna	Medici di base, specialisti, CM SERVICE	C
7.p	Registro delle consegne	C	S	Personale OSS	CM SERVICE SRL, Medici e Infermieri	C
8.c	Dati sanitari ospiti per pasti	C	S	Esterna	CM SERVICE SRL	C

9.l	Lavanderia	C		Esterna	CM SERVICE SRL	C
10.lv	Elaborazione Paghe	C	S	Ufficio Amministrativo	ENTI SERVICE	C
11.a	Protocollo	C	S	Ufficio Amministrativo	CBA INFORMATICA SRL	I

Le strutture all'interno dell'organizzazione complessiva della Casa di Riposo di Bricherasio che si occupano del trattamento di dati personali, anche in relazione ai compiti loro assegnati sono le seguenti:

Tabella 2.1: Strutture interne preposte ai trattamenti

Struttura	Interna/ Esterna	Eventuale Responsabile	Trattamento operati dalla struttura	Compiti della struttura
Ufficio Amministrativo	I		1.a, 2.a, 3.a, 4.a, 5.a, 11.a	Adempimenti amministrativi di ogni genere, sia verso l'interno che verso l'esterno
Personale OSS	I		7.p	Assistenza generica ospiti

4. DISTRIBUZIONE DEI COMPITI

In base alla valutazione dei rischi ed all'esame della tipologia, dell'entità e della distribuzione delle attività condotte dalla Casa di Riposo di Bricherasio nell'attuazione dell'attività lavorativa della propria organizzazione:

- ciascun dipendente e collaboratore è stato esplicitamente incaricato ed autorizzato, mediante apposito provvedimento di Incarico, al trattamento dei diversi tipi di dati;
- gli incarichi – così come la responsabilità per la conservazione dei dati – vengono conferiti personalmente al momento dell'inserimento di una nuova figura all'interno della struttura dell'ente;
- ciascun Incaricato può operare, per il trattamento dei dati, esclusivamente all'interno delle mansioni assegnate e in riferimento alle informazioni ed alle Banche dati disponibili relative

alla propria categoria di appartenenza;

- i soggetti che trattano dati riferiti all'attività della Casa di Riposo, ma che, per qualifica attribuita, od in relazione alla concreta attività svolta, non rivestono la figura di Incaricati, sono stati opportunamente autorizzati al trattamento, mediante specifica Convenzione che riguarda l'utilizzo dei dati e le diverse responsabilità di ognuno, come esaminato nel seguito del presente paragrafo.

L'attuale organizzazione interna della struttura, sempre in relazione ai soggetti coinvolti nel trattamento di dati rilevanti ai fini del Testo Unico, è la seguente:

- *Collegio Commissariale della Casa di Riposo.* Tale organo non ha poteri diretti di gestione delle banche dati, né opera eseguendo trattamenti. Tuttavia, al fine di svolgere appieno il mandato loro conferito, ogni amministratore ha poteri di consultazione di ogni documento, sia cartaceo che informatico, anche contenente dati sensibili;
- *Ufficio Amministrativo* formato da n. 1 soggetto, sig.ra. Martina Marisa, Direttore della Casa di Riposo. Tale soggetto opera in relazione agli specifici incarichi assegnati utilizzando le Banche dati di riferimento, così come documentato nel precedente paragrafo;
- *Personale assistenziale interno* formato attualmente da n. 2 OSS. Tali dipendenti dell'Ente operano in relazione agli specifici incarichi assegnati utilizzando le Banche dati di riferimento, così come documentato nel precedente paragrafo. Le modalità di trattamento saranno esplicitate nel seguito del presente DPS.

In relazione a quanto è necessario stabilire con il presente DPS, vanno segnalati diversi soggetti che, pur non essendo alle dipendenze della struttura, anche in considerazione di quanto segnalato alla Tabella 1.1 di questo documento, partecipano attivamente al trattamento di dati rilevanti ai fini del Testo Unico sulla Privacy. Tali soggetti agiscono in base a specifici incarichi od appalti, oppure, come nel caso dei Medici, in relazione ad obblighi che norme di legge loro impongono; la seguente tabella documenta l'attuale situazione della Casa di Riposo in relazione ai soggetti esterni alla struttura.

Tabella 3.1: Strutture esterne preposte ai trattamenti (anche eventuali)

Struttura	Attività	Trattamenti in cui interviene il soggetto	Motivo dell'intervento
CM SERVICE SRL	Servizio socio-Assistenziale notturno e diurno	7.p	Appalto
	Lavanderia, Cucina, Pulizie, Fattorino, animatrice	8.c, 9.l	
	Fisioterapia, infermieri, Psicologo	6.i, 7.p	
CBA Informatica srl di Rovereto	Assistenza programmi contabilità/mandati reversali/protocollo/ rilevazione presenze	1.a, 11.a	Utilizzo programmi
Centro Servizi Environment & Health di M. Gerbaldo	Incarico Direttore Sanitario	6.i	Incarico
Dott. Longo Vaschetto Luca	Sostituto Diretto Sanitario	6.i	Incarico
Medico di base	Scheda sanitaria per inserimento ospite	3.a	Richiesta assistito
Medico di base	Aggiornamento cartella clinica, PAI	6.i	Visita assistito
Medico specialista	Aggiornamento cartella clinica	3.a, 6.i	Visita od esame ospite
Medico 118 o guardia medica	Interventi di urgenza		Visita od esame ospite
Amico Anziano	Volontari (Assistenza ospite)		Incarico

E-Public Srl	Assistenza sito internet		Incarico
Paolo Beda	Assistenza Hardware		Incarico

In dettaglio, il coinvolgimento dei predetti soggetti esterni, è il seguente:

- *Ditta che effettua attività di assistenza socio-sanitaria, infermieristica*. Attualmente la struttura affida alla CM SERVICE SRL il servizio di assistenza da effettuare in collaborazione con le OSS dipendenti dirette della Casa di Riposo. Il contratto di affidamento disciplina l'attività richiesta, mentre ai fini della disciplina della Privacy viene redatta un'apposita nomina.
- *Ditta che svolgono attività di pulizia dei locali e gestione e somministrazione pasti*. Anche tale servizio è affidato alla CM SERVICE SRL . Valgono le medesime precisazioni sulla circostanziata indicazione delle responsabilità e del controllo sulle prestazioni ricevute di cui al punto precedente. La Ditta incaricata delle pulizie dei locali può operare sotto il controllo di dipendenti dell'Ente, od in locali in cui il/i lavoratore/i è/sono temporaneamente solo/i, e ciò potrà avvenire in qualsiasi ambiente. L'Autorizzazione conferita tiene specificatamente conto di questa modalità organizzativa, sottolineando l'ambito e la disciplina delle responsabilità a cui si va incontro. La gestione della somministrazione e della preparazione dei pasti è effettuata dalla medesima ditta. A tale scopo il personale di cucina riceve informazioni puntuali e dettagliate su particolari problematiche sanitarie, o determinate disfunzioni temporanee degli ospiti. Pertanto la CM SERVICE SRL deve adeguatamente istruire i propri dipendenti sui limiti e sui divieti di comunicazione e diffusione dei dati stabiliti dalla legge. Anche questo tipo di indicazione è dettagliatamente segnalato nell'autorizzazione conferita;
- *Società, ditte e Liberi Professionisti che effettuano la manutenzione dei Personal computers, dei software e delle reti informatiche e/o elaborazione dati*. Tali soggetti operano in base a specifica autorizzazione, recante nel dettaglio compiti e i limiti nell'espletamento dell'attività di assistenza. In particolare, queste Ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione, o semplicemente è necessario verificare il funzionamento di un programma o di una attrezzatura informatica. A tal fine è praticamente obbligatorio accedere alle base di dati presenti sui personal computers o all'interno dei programmi software, evidenziando così una conoscenza di dati personali che di per sé, non è collegata

allo scopo per cui la Ditta effettua la propria attività. Pertanto l'autorizzazione/accordo concluso con ognuno di questi soggetti indicherà i limiti e le responsabilità a cui la Ditta andrà incontro nel caso in cui i dati accidentalmente conosciuti vengano comunicati o diffusi in violazione della normativa sulla Privacy. Si precisa che naturalmente non sarà posta in essere alcuna violazione di legge qualora all'interno della prestazione offerta da queste Ditte siano comprese anche determinate attività di elaborazione dati. In particolare l'attività di elaborazione paghe comporta il trattamento dei dati da parte della ditta ENTI SERVICE SRL che ha assunto il ruolo di titolare autonomo del trattamento dati, senza necessità di ulteriori accordi con il Ns. Ente, in considerazione delle maggiori responsabilità connesse a tale figura;

- *Direttore Sanitario*. Detta attività è affidata, mediante incarico libero professionale, al Dott. Varetto Henry, medico avente idonei titoli sanitari e professionali ed in relazione agli specifici incarichi assegnati utilizzando le Banche dati di riferimento, così come documentato nel precedente paragrafo;
- *Medici di base, specialisti, Guardia Medica e 118*; i predetti soggetti operano in relazione a situazioni anche relativamente diverse, ma tutti con la specifica finalità dell'assistenza medica e sanitaria dei soggetti ospiti della Casa di Riposo. Naturalmente il rapporto con il Medico di Base non discende direttamente dal fatto di essere ospite della struttura, ma esiste per ogni persona; però dal momento in cui un soggetto diventa un utente della Casa di Riposo, l'attività del Medico di Base si interseca con determinati adempimenti da porre in essere in collaborazione con l'Ente. In particolare il Medico attesta la condizione fisico-psicologica del soggetto che richiede di entrare a far parte della struttura, dopodichè provvede ad aggiornare la cartella sanitaria che viene conservata all'interno dei locali della Casa di Riposo.

  I Medici specialisti si occupano di visitare gli ospiti presso la struttura della Casa di Riposo, o, più frequentemente, presso il proprio studio professionale o comunque in altro luogo al di fuori dello stabile dell'Ente, al fine di provvedere ad espletare l'attività per la quale sono stati consultati. Questi soggetti ricevono e consultano la documentazione attestante vari aspetti della condizione sanitaria dell'ospite, necessaria ad una corretta disamina della situazione, e procedono a rilasciare i risultati dell'esame; la loro attività si conclude ed è circoscritta nell'ambito della prestazione richiesta, e, pertanto può essere svolta anche senza alcun tipo di accordo tra la Casa di Riposo ed il Medico specialista. Allo stesso modo, seppure per motivazioni di urgenza e quindi con diverse finalità, va individuato il rapporto nei confronti

del personale di Guardia Medica e del 118. Questi medici hanno la assoluta necessità di conoscere a fondo la condizione sanitaria della persona che necessita di cura ed assistenza, ed è quindi corretto comunicare loro ogni dato ed informazione concernente lo stato di salute, senza obbligo di stipula di alcun accordo preventivo o successivo.

- *Volontari*; in relazione alle finalità assistenziali e sociali della Casa di Riposo, esistono dei soggetti che operano a favore degli ospiti prestando la loro attività volontariamente, che appartengono all'associazione "Amico Anziano". Queste persone si occupano di vari e diversi ambiti dell'attività dell'Ente, sia nel campo dell'aspetto ricreativo (animazione, ecc.), sia nell'assistenza alla somministrazione dei pasti. Tutte queste attività variano in relazione alle esigenze della struttura e, naturalmente, anche in base alla disponibilità dei volontari. Ai fini della disciplina della privacy, la collaborazione dei volontari diventa rilevante nel momento in cui, anche accidentalmente, si deve venire a conoscenza di alcuni dati relativi agli ospiti. Per questa ragione l'Associazione "Amico Anziano" opera in base a specifica autorizzazione, che dovrà essere riferito alle effettive attività svolte e tutti i limiti ed i profili di responsabilità che riguardano ogni eventuale trattamento.
- *Amministratori di Sistema.* secondo quanto stabilito con provvedimento del 27 novembre 2008 da parte del Garante per la protezione dei dati personali, è colui che "professionalmente si occupa di gestione e manutenzione di un impianto di elaborazione o di sue componenti" oppure "è un amministratore di basi di dati, di reti e di apparati di sicurezza o ancora è un amministratore di sistemi software complessi". In base a queste definizioni, ed anche in base a quanto previsto dalle precisazioni del Garante stesso con provvedimento del 10 dicembre 2009, l'Ente ha proceduto ad individuare e nominare con apposito documento Amministratori di Sistema coloro che si trovino nelle posizioni testè evidenziate. Nella comunicazione di nomina sono stati espressamente indicati gli elementi caratterizzanti la nomina, indicando gli obblighi conseguenti. Tutti i soggetti indicati avevano già ricevuto l'indicazione sulle modalità di espletamento delle proprie attività connesse ai diversi incarichi di lavoro attribuiti; la nomina ad Amministratore di Sistema è da considerare quale integrazione.

La seguente tabella riassume il soggetto nominato, con indicazione sintetica delle attività svolte:

NOME ADS	Attività
Beda Paolo	Assistenza hardware

Tutti i soggetti sinora elencati, in relazione a quanto specificato per ognuno di essi, sottoscrivono un accordo con la Casa di Riposo che disciplina esattamente gli ambiti di responsabilità e di obblighi che le parti sono tenute ad assumere e che si impegnano ad effettuare. Tutte le Ditte ed i soggetti che operano attraverso propri dipendenti e collaboratori si obbligano a rendere edotti queste persone di tutto quanto previsto dagli accordi ed in generale dalla normativa sulla privacy. Da queste intese sono esclusi, in quanto rientrano in attività specialistiche e di emergenza sanitaria effettuate in relazione a specifici obblighi, i medici specialisti, i medici del 118 ed il personale di Guardia Medica.

L'affidamento all'esterno (outsourcing) di parti di attività di trattamento dati relativi alla Casa di Riposo di Bricherasio comporterà l'obbligo, identificato specificatamente all'interno del contratto di servizio o di elaborazione, da parte del terzo di applicazione dell'intera normativa sulla privacy, sia, a puro titolo esemplificativo in relazione alle modalità di trattamento e comunicazione dei dati, sia soprattutto in relazione alle Misure di Sicurezza.

5. DISPOSIZIONI SULL'ACCESSO AI LOCALI ED AI DATI PERSONALI

Poiché il rischio da eliminare riguarda il potenziale trattamento o la conoscenza di dati personali da parte di soggetti non autorizzati, evidenziamo le disposizioni sull'accesso ai locali della Casa di Riposo di Bricherasio da parte di altri soggetti (utenti, famigliari e conoscenti degli ospiti, tecnici e manutentori, ecc.), che riguardano le misure di sicurezza minime che la struttura attualmente applica.

A) MISURE DI SICUREZZA FISICHE

Richiamando, per una parte delle informazioni necessarie, le indicazioni fornite all'inizio del presente Documento sulla sicurezza, dettagliamo altre Misure specifiche relative ai locali ed agli Uffici in cui la conservazione ed il trattamento dei dati personali assumono una importanza rilevante.

Accesso ai locali

Gli accessi alle parti comuni dell'edificio devono essere chiusi (a chiave nel caso delle porte)

negli orari in cui la Casa di Riposo non ha personale che vigila sull'accesso dall'esterno, tenendo conto che la continua presenza di addetti, anche in orario notturno, permette di ridurre notevolmente il rischio di intrusioni sconosciute. Negli orari di apertura al pubblico, nessun dato personale deve essere posto in vista, o deve essere facilmente accessibile o riconoscibile a chiunque.

Si richiamano inoltre le disposizioni già segnalate nel secondo paragrafo relativo all'Analisi dei Rischi. Vediamo ora le disposizioni riguardanti specifici locali:

- ***Uffici Amministrativi***

L'accesso agli Uffici amministrativi è strettamente controllato da parte degli Incaricati che effettuano trattamenti di dati personali. Durante il normale orario di apertura degli Uffici, l'accesso ai dati è controllato dai rispettivi incaricati e qualora, per motivi diversi, un Ufficio rimanga temporaneamente vuoto, l'incaricato è obbligato a chiudere a chiave la porta d'accesso dello stesso e custodire la copia di chiavi che ne permettono l'apertura (ovvero consegnarla al collega o ad altro soggetto che comunque abbia diritto ad espletare la propria attività nel medesimo Ufficio).

In ogni caso, ciascun incaricato deve rendere i dati personali specificamente trattati non consultabili o visibili da parte di eventuali terzi che abbiano diritto ad accedere all'Ufficio né al collega che stia svolgendo il proprio lavoro nel medesimo locale. I terzi che possono accedere agli Uffici negli orari di apertura e/o di chiusura sono espressamente determinati in apposite autorizzazioni loro conferite, nelle quali sono indicate le responsabilità loro riferite, quale ad esempio il personale di pulizia, come già evidenziato nel precedente paragrafo.

Tutti gli incaricati devono provvedere a non lasciare mai, in loro assenza, porte e finestre dei rispettivi Uffici aperte. Gli accessi specifici (cassetti, armadi, ecc.) vanno chiusi a chiave sempre, le porte solo in assenza degli addetti dai rispettivi Uffici. Tutti i dati sensibili contenuti su documenti cartacei (quale ad esempio il libretto sanitario) devono sempre essere conservati dentro armadi o contenitori chiusi a chiave, cosa che viene correttamente adempiute tramite apposito schedario con chiusura di sicurezza.

- ***Infermerie***

L'infermeria è il locale che i Medici di norma utilizzano per effettuare le visite periodiche agli ospiti, e dove inoltre vengono conservati i medicinali da somministrare, nonché le cartelle

cliniche. Sia le cartelle cliniche, che altre informazioni sanitarie che riguardano gli ospiti, come ad esempio radiografie e quant'altro, devono essere conservate in contenitori chiusi a chiave, od in raccoglitori chiusi con dei lucchetti. L'accesso al locale Infermeria è riservato alle Infermiere e agli operatori di settore che operano all'interno della struttura, qualunque sia il loro inquadramento.

Una chiave del locale Infermeria è conservata nell'Ufficio Amministrativo per eventuali emergenze, così come è disponibile una chiave di accesso da parte del personale che svolge assistenza notturna, da utilizzare sempre in caso di emergenza. Tali utilizzi eccezionali, vanno comunicati al Direttore della Casa di Riposo, esponendo anche le motivazioni che hanno portato all'apertura del locale, ed all'eventuale trattamento o comunicazione di dati sanitari ricavati dalle cartelle cliniche o da altri documenti.

- ***Cucinotta***

All'interno della struttura esiste un locale denominato cucinetta, situato al primo piano, ove, oltre ad alcuni alimenti e stoviglie, sono conservati alcuni documenti rilevanti ai fini della normativa sulla privacy. In particolare ci si riferisce al Registro delle consegne, utilizzato dal Personale di assistenza, ove vengono segnalate tutte le informazioni necessarie all'espletamento di un corretto servizio di aiuto e cura nei confronti degli ospiti, che il personale e la CM Service convenzionata, in occasione del passaggio di turno ritiene utile comunicare.

In assenza di Incaricati che sorvegliano l'accesso al locale, esso deve essere chiuso, a meno che tutte le informazioni (il Registro ed eventuale altra documentazione) vengano temporaneamente utilizzate da altre parti, come ad esempio per la consultazione o la compilazione del Registro. Al di fuori degli orari di assistenza diurna normali, i locali verranno di norma chiusi; saranno aperti ed utilizzati solamente da chi svolge l'assistenza notturna, mantenendo il controllo sull'entrata in modo da non rendere conoscibile alcun dato.

Istruzione per Trattamenti dati cartacei:

In relazione alle Misure di Sicurezza Fisiche, si ritiene fondamentale evidenziare le istruzioni al trattamento riguardanti la complessiva attività della Casa di Riposo, la cui applicazione pratica risulta essere di vitale importanza per la concreta applicazione del presente Documento. In particolare tutte le informazioni riportate su documenti cartacei, delle quali si abbia effettiva esigenza di consultazione, devono essere prelevate e detenute in base alla loro attinenza e pertinenza con il trattamento richiesto.

Gli archivi sono ad accesso selezionato, cioè è possibile ricercare ed estrarre esclusivamente i dati necessari per il trattamento. Se si tratta di dati sensibili o giudiziari, ai sensi dell'art. 4, comma 1, lettere d) ed e) del Testo Unico, gli incaricati devono utilizzare esclusivamente i dati strettamente necessari allo svolgimento delle proprie mansioni ed immediatamente restituirli al termine delle operazioni.

I dati sensibili e giudiziari, così come sopra definiti, devono essere conservati dentro contenitori muniti di serratura. Se una o più informazioni devono rimanere a disposizione per un trattamento prolungato o continuo, l'incaricato deve essere sempre presente nel locale ove avviene il trattamento ed essere in grado di impedire a terzi di vedere la documentazione in uso. Nel caso in cui sia indispensabile l'accesso al locale da parte di terzi, l'incaricato provvede preventivamente a riporre tutti i dati personali in consultazione nei relativi siti protetti.

Tutti i soggetti, interni o esterni all'ente, che possono accedere all'edificio o anche ai dati cartacei sono muniti di esplicita autorizzazione, recante in dettaglio le regole per il corretto trattamento dei dati e/o i limiti e le responsabilità connesse al loro diritto di accesso. Tali autorizzazioni sono periodicamente controllate, al fine di verificare la loro osservanza ed adeguatezza alle condizioni di espletamento dei servizi ed in relazione alle motivazioni per le quali sono state assegnate.

B) MISURE DI SICUREZZA INFORMATICHE

Si riportano le principali misure di sicurezza da utilizzare nel trattamento informatico dei dati, che devono essere seguiti da tutti i soggetti coinvolti nell'attività della Casa di Riposo. Tali comportamenti riguardano sia l'ambito strutturale minimo che i sistemi informatici devono possedere, sia l'ambito delle istruzioni che sono state fornite ai diversi incaricati di ogni settore.

Attualmente gli strumenti informatici utilizzati sono due Personal computers di cui solamente uno tratta dati personali, ed è usato dal personale Amministrativo.

Le indicazioni che vengono evidenziate con il presente documento riguardano l'attuale dotazione informatica dell'Ente, ma dovranno essere comunque prese a riferimento anche in relazione a variazioni che ne modifichino la configurazione, come ad esempio la creazione di una rete informatica, o l'aggiunta di nuovi Personal Computers.

Istruzione per Trattamenti dati informatici

Le parole chiave di qualunque tipo devono rispettare le seguenti regole generali. Esse:

- devono essere composte da almeno 8 caratteri alfanumerici;
- non devono essere nomi di persona, né date di nascita;
- gli incaricati devono adottare le dovute cautele per assicurare la segretezza di ogni password assegnata. Devono altresì garantirne l'aggiornamento tempestivo e la disponibilità, se la password viene utilizzata da più soggetti, oppure se deve essere conservata al fine di rendere possibile un intervento in caso di prolungata assenza o impedimento che renda indispensabile e indifferibile intervenire sul sistema per esclusive necessità di operatività e di sicurezza;

Altre regole più specifiche verranno segnalate in relazione a determinati ambiti di utilizzo delle parole chiave.

A tutela delle informazioni contenute su supporti informatici e derivanti da trattamenti compiuti per mezzo di elaboratori sia in rete che non, si dispone la predisposizione, per ciascun personal computer in uso, di una parola chiave all'accensione dello stesso (password di BIOS), conosciuta dagli utenti della specifica postazione di lavoro. Sono tali i soggetti che operano all'interno del medesimo locale, o che per esigenze di consultazione dei dati, hanno necessità che un determinato personal sia acceso per poter esaminare una serie di informazioni essenziali per uno specifico trattamento.

Su ogni computer, in rete o meno, deve inoltre essere attivata la funzione di oscuramento o copertura con decorazioni di quanto visualizzato sul monitor, in assenza dell'operatore (screen saver): essa deve essere impostata in modo da entrare in azione in assenza di input per un periodo al massimo pari a 5 minuti e richiedere una parola chiave per essere disattivata. Tale parola chiave, soprattutto nel caso di elaboratori non in rete ad uso promiscuo, deve essere nota a tutti gli utenti della postazione, così come prima definiti.

Sia la password di BIOS che la password di screen saver devono unicamente seguire le regole minime di determinazione delle parole chiave, di cui in precedenza.

Tutti gli elaboratori devono essere protetti da programmi anti-virus contro il rischio di intrusione ad opera di virus informatici, che potrebbero essere introdotti inavvertitamente anche dal personale interno, mediante inserimento di supporti di memoria (floppy disk, cd-rom ed altro). La costante attività di tali programmi deve essere verificata almeno semestralmente e

almeno in tali occasioni si procede all'aggiornamento degli stessi.

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale (anti-virus). Nel caso di trattamento informatico di dati sensibili o giudiziari deve essere attivata la protezione contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici (firewall).

In relazione alle modalità di trattamento dei dati, tutte le informazioni che vengono temporaneamente salvate su supporti rimovibili (es. floppy disk) sono trattate sotto la totale responsabilità degli incaricati, i quali dovranno provvedere alla loro conservazione dentro contenitori chiusi a chiave, provvedendo eventualmente a dei doppi salvataggi per evitare la perdita dei dati.

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili. Allo stesso modo gli incaricati non possono portare al di fuori dell'edificio tali supporti e, qualora questi ultimi contengano dati sensibili, sono tenuti a formattarli, purché i dati stessi siano stati registrati – se necessario - nella memoria fissa degli elaboratori e non si debba disporre di una copia su supporto rimovibile, che va comunque conservata nei cassetti ed armadi chiusi a chiave, analogamente ai dati cartacei. Ogni utilizzo o trasporto all'esterno di questi supporti è solamente ammesso per esigenze di semplificazione e di immediatezza dei trattamenti, ma è effettuato sotto la piena e totale responsabilità degli Incaricati.

Per l'utilizzo dei programmi dedicati e della rete informatica è assegnata ad ogni utente una o più credenziali di autenticazione che, oltre a seguire le regole delle parole chiave di cui sopra, devono avere le seguenti caratteristiche e devono essere utilizzate nel seguente modo:

- la credenziale è una sola nel caso in cui il soggetto incaricato viene unicamente identificato al momento del suo ingresso nella rete, con una sua configurazione che gli permette l'accesso ai propri programmi e documenti relativi alle mansioni assegnate;
- la credenziale è più di una nel caso in cui il soggetto va identificato nel momento di accesso a più programmi specifici che necessitano singolarmente di una password. Se il programma è uno solo, o i programmi da utilizzare e consultare possono ricomprendere una

configurazione unica, la credenziale rimane unica;

- la/e credenziale/i di autenticazione devono essere di almeno 8 caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito e non deve essere banale né facilmente riconducibile al soggetto a cui è/sono assegnata/e;
- l'incaricato è tenuto a modificare la/e credenziale/i di autenticazione al primo utilizzo e successivamente almeno una volta ogni trimestre;
- dovute cautele devono essere adottate per assicurare la segretezza della componente riservata della/e credenziale/i assegnata;
- è garantita la massima segretezza – secondo le modalità operative concordate col titolare/responsabile – nell'accesso ai dati o strumenti elettronici da parte di terzi in caso di prolungata assenza o impedimento che renda indispensabile e indifferibile intervenire sul sistema per esclusive necessità di operatività e di sicurezza;
- la medesima credenziale di autenticazione, per quanto riguarda il codice per l'identificazione, non può essere assegnata 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.

Il codice per l'identificazione deve essere composto da caratteri alfanumerici, ma può contenere alcuni o tutti gli elementi del nome e cognome del destinatario.

Ulteriori istruzioni riguardano il salvataggio dei dati che deve essere effettuato con frequenza almeno settimanale. Il salvataggio avviene su disco fisso in maniera da garantire al meglio la disponibilità dei dati nel caso in cui sopraggiungessero problemi relativi all'utilizzo degli strumenti informatici o della rete che impedisca il trattamento dei dati. In caso di danneggiamento dei dati o degli strumenti elettronici in modo definitivo, le procedure di ripristino danno la garanzia di ripristinare l'accesso ai dati in tempi non superiori a sette giorni.

6. PREVISIONE DI INTERVENTI FORMATIVI

Gli incaricati del trattamento, ai sensi del punto 19.6 del Disciplinare Tecnico allegato al Testo Unico, devono essere adeguatamente formati al fine di essere resi 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 e delle responsabilità che ne derivano.

Gli interventi formativi dovranno essere posti in essere nei confronti di ogni incaricato almeno annualmente, secondo modalità e metodologie che verranno stabilite in relazione alle mansioni ed alle caratteristiche specifiche del soggetto coinvolto nella formazione.

In sede di prima applicazione della misura, ogni incaricato dovrà comunque documentare di aver adempiuto all'obbligo formativo, nell'arco di un anno e mezzo successivi all'approvazione del presente DPS. Successivamente l'obbligo di formazione sarà annuale. I nuovi assunti, le cui mansioni saranno rilevanti ai fini del trattamento dei dati personali, dovranno adempiere all'obbligo almeno entro i dodici mesi dall'entrata in servizio.

Nel caso di introduzione di nuovi significativi strumenti legislativi o di qualunque genere che rivestano comunque un rilevante rispetto alla materia del trattamento di dati personali, la formazione dovrà essere garantita agli interessati nel tempo massimo di sei mesi dall'evento.

CONCLUSIONI ED ISTRUZIONI PER L'AGGIORNAMENTO DEL DPS

Le misure di sicurezza descritte, in relazione all'attuale organizzazione anche informatica della Casa di Riposo, risultano interamente applicate alla data di redazione del presente documento.

Il presente DPS sarà qualora intervengano fatti rilevanti relativi all'organizzazione della Casa di Riposo, od altri fatti comunque ritenuti importanti, il documento verrà aggiornato senza indugio. In tutti i casi l'aggiornamento potrà essere effettuato anche soltanto per mezzo di richiamo ad integrazione della presente scrittura.

Luogo e data

Il Legale Rappresentante