Casa di Cura Privata "DI LORENZO" spa
Direttore Sanitario: Dott. Angelo Petroni
Via Vittorio Veneto, 37 67051 Avezzano (Aq)
tel 0863 4281 fax 0863 412446 e-mail: info@dilorenzo.it www.dilorenzo.it

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Società: Casa di Cura Privata Di Lorenzo s.p.a., con sede legale in Avezzano (AQ), Via Vittorio Veneto, n° 37.

Data di revisione: 24 luglio 2018 (13^ redazione)

Approvato da: Lucia Di Lorenzo (Titolare del trattamento)

INDICE

1. Premessa

La Casa di Cura Privata Di Lorenzo S.p.A., in questo documento per convenzione denominata anche "DL", ha provveduto (in ossequio a quanto previsto dal punto 19 del "Disciplinare Tecnico in materia di misure minime di sicurezza" allegato al D. Lgs. n. 196/2003) a redigere per l'anno 2005, il Documento Programmatico sulla Sicurezza contenente idonee informazioni riguardo e a procedere con cadenza annuale alla sua revisione in merito a:

- 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 ed accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino delle disponibilità dei dati in seguito a distruzione o danneggiamento dei medesimi o degli strumenti elettronici;
- 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;

Il presente documento costituisce l'aggiornamento per l'anno 2018 del DPS aziendale che, pur non necessitando più di redazione/aggiornamento e relativa data certa (*ai sensi dell'art. 45 del Decreto semplificazioni n° 5 del 09/02/2012*), viene ugualmente revisionato con cadenza almeno biennale; sia per accertare l'adeguamento normativo (es.: recepimento regolamenti Garante, Nuovo Regolamento Europeo, Disciplina del DSE Dossier Sanitario Elettronico ecc.), sia per accertare il permanere di tutte le condizioni di sicurezza ivi previste. L'adeguamento 2018 in particolare tiene conto dell'entrata in vigore del Regolamento Europeo per la Privacy (GDPR) e di tutti i documenti e nuove nomine richiesti da tale nuova normativa.

Si riportano di seguito le principali variazioni rispetto alla precedente edizione:

1. Rivalutazione e integrazione elenco responsabili esterni al trattamento
2. Recepimento indicazioni del regolamento Europeo e programma di adeguamento
3. Nomina DPO
4. Sostituzione del server e rinnovo PC
5. Istituzione server di dominio
6. Collegamento con il Registro dei trattamenti
7. Rinnovo documentazione incarichi privacy
8. Revisione delle informative e dei consensi per adeguamento al GDPR
9. Miglioramento sistemi di sicurezza
10. Introduzione data breach
11. Aggiornamento piano formativo

Il presente documento (chiamato anche DPSS) definisce le procedure di gestione della Privacy e le misure adottate da DL per la sicurezza dei sistemi informativi e degli archivi documentali elettronici e non.

Il presente DPSS è stato divulgato a tutto il personale della Società e dalla stessa applicato, tramite affissione in bacheca e pubblicazione su PC contenente i documenti condivisi.

La sicurezza dei sistemi informatici e di telecomunicazione viene definita come la "protezione dei requisiti di integrità, disponibilità e confidenzialità" delle informazioni trattate, ossia acquisite, comunicate, archiviate, processate, dove:

- integrità è la proprietà dell'informazione di non essere alterabile;
- disponibilità è la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati, per le finalità indicate ed il tempo massimo definito;
- confidenzialità è la proprietà dell'informazione di essere nota solo a chi ne ha il diritto in base ai presupposti giuridici del trattamento.

Per le informazioni e i sistemi connessi in rete le esigenze di sicurezza includono anche:

- autenticità, ossia la certezza da parte del destinatario dell'identità del mittente;

La sicurezza dei sistemi informatici e degli archivi si estrinseca in una politica ed in un piano operativo che fa riferimento agli aspetti di protezione e agli aspetti di emergenza.

Metodologia Applicata

Si è provveduto a censire i trattamenti di dati effettuati in azienda secondo quanto previsto dal GDPR istituendo il registro dei trattamenti come definito, sia per il titolare che per il Responsabile del trattamento.

Le attività effettuate per la scrittura del presente Documento programmatico sono state:

- censire tutte le misure di sicurezza poste a tutela dei singoli trattamenti;
- individuare in modo formalizzato le persone fisiche autorizzate ai diversi trattamenti;
- definire i profili di accesso ai sistemi;
- valutare le misure di sicurezza adottate, verificando la loro corrispondenza con quanto previsto dal Codice Privacy e dal GDPR
- descrivere la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

Sono stati individuati e valutati i seguenti rischi: distruzione e perdita, anche accidentale, dei dati, accessi non autorizzati, trattamenti non consentiti o non conformi rispetto alle finalità della raccolta, tempi di conservazione dei dati.

L'analisi dei rischi ha riguardato i sistemi informatici e telematici; non sono ad oggi attivi sistemi di registrazione telefonica e/o di videosorveglianza.

Il Documento Programmatico della azienda si riferisce ai trattamenti di dati sensibili (in particolare quelli idonei a rilevare lo stato di salute delle persone) svolti direttamente dalla medesima con l'ausilio di strumenti elettronici, con personale e mezzi propri, nell'ambito delle proprie strutture.

Infine, é stato definito un piano di formazione degli incaricati del trattamento.

2. Elenco dei trattamenti – Registro dei trattamenti

Per l'elenco dei trattamenti, i contitolari ed i responsabili esterni, si fa rinvio al registro dei trattamenti.

3. Distribuzione dei compiti e delle responsabilità

Titolare del trattamento dei dati è la Casa di Cura Privata "Di Lorenzo" Spa nella persona del suo rappresentante legale.

É stata disposta la distribuzione dei compiti e delle responsabilità previste nell'ambito della struttura aziendale con riguardo alla gestione dei rischi connessi al trattamento di dati personali nonché ai controlli effettuati in materia.

In particolare, sono stati presi in considerazione i trattamenti dei dati personali svolti con strumenti elettronici.

3.1. La struttura aziendale

DL ha definito un assetto organizzativo deputato a garantire la gestione della privacy nonché della sicurezza fisica, logica ed organizzativa.

3.1.1. Incaricati del trattamento dei dati

Tutto il personale dipendente che svolge operazioni di trattamento di dati personali è stato preventivamente individuato e ne sono stati designati i responsabili/coordinatori, con specifico incarico, all'uopo delegati che hanno ricevuto istruzioni dal Titolare dei trattamenti. Sono stati rinnovati tutti gli incarichi ai Responsabili del trattamento (o incaricati) per adeguamento al GDPR.

3.1.2. Responsabili del trattamento dei dati personali

Il Responsabile interno del trattamento dei dati personali è il Direttore Amministrativo Sig.ra Patrizia Iacoboni.

I Responsabili esterni del trattamento dei dati sono: ASL 1 Abruzzo L'Aquila; DEDALUS s.p.a. (anche per dati sensibili); **Project Innovation s.r.l.** (anche per i dati sensibili); Synlab (ex Fleming Labs) e Guidonia (ex ADI), SSR Emilia Romagna per fornitura di tessuti; Studio Associato Giacobini-Davola e Studio Manerin per dati contabili, fiscali e anagrafiche dipendenti (dati personali); CSP s.r.l. per la gestione, la custodia e la scannerizzazione e trasmissione telematica del contenuto delle Cartelle Cliniche; Sofar o altro fornitore equivalente e qualificato dei test, per la gestione dei referti dei breath test. Tali Responsabili hanno ricevuto e firmato per accettazione la lettera di incarico, con le modalità per il corretto svolgimento dell'attività ***ed è in corso di predisposizione la revisione della stessa per adeguamento al GDPR e la verifica che tutti si siano dotati del registro dei Trattamenti. E' inoltre in corso di valutazione la posizione della ASL1 Abruzzo se da definire in qualità di responsabile esterno del trattamento o di contitolare. Siamo in attesa di riscontro dalla ASL.***

Per quanto concerne la ASL 1 Abruzzo ed il SSR Emilia Romagna: Banca del Tessuto Muscolo-scheletrico (per il tramite dell'Ospedale dell'Aquila), essendo parte stessa del SSN, il dato è considerato interno ai fini del trattamento dei dati sensibili e non necessita pertanto di apposite ulteriori autorizzazioni e/o liberatorie del paziente o dell'Ente.

3.1.3. Gestione della sicurezza logica, organizzativa e fisica

Responsabile per la gestione della sicurezza logica ed organizzativa nonché incaricato della corretta tenuta delle copie di sicurezza è il Sig. Domenico Canerossi.

In assenza del Sig. Domenico Canerossi, è stato designato come sostituto per le funzioni attribuite il Dott. Maurizio Gentile, che ha sottoscritto idonea lettera di incarico. E' stata inoltre incaricata della gestione dell'infrastruttura informatica della Società Di Lorenzo la Project Innovation s.r.l., con la quale è stato stipulato apposito contratto come definito dal GDPR.

I compiti sono i seguenti:

- garantire la sicurezza, l'integrità e la riservatezza dei dati;
- controllare l'assegnazione dei profili di l'accesso al sistema informativo.

Le parole chiave di accesso al sistema sono assegnate dal Sig. Domenico Canerossi, conservate sul sistema con chiave di accesso detenuta dal Sig. Domenico Canerossi e dal Titolare del trattamento. Una copia dell'elenco dei detentori di password con date di validità è stampata e conservata con cadenza annuale dal responsabile del trattamento e custodita in cassaforte presso l'ufficio del DA, unitamente all'elenco delle password di sistema. In ogni caso l'elenco è sempre consultabile sul sistema Dedalus aggiornato in tempo reale.

Il Sig. Domenico Canerossi, provvede inoltre:

- alla prima assegnazione delle password agli utilizzatori;
- alla modifica, disattivazione, riattivazione di password per utenti che sono temporaneamente assenti, che hanno cessato il rapporto con la Casa di Cura o che hanno dimenticato la password, secondo le istruzioni operative del sistema (utilizzo del super user).

Il sig. Domenico Canerossi inoltre è stato nominato Amministratore di Sistema. Specificatamente e limitatamente a tale contesto i suoi compiti consistono in:

- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte Sua (nella sua qualità di "amministratore di sistema"); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Il Dott. Gabriele Pizzi Scatena è stato nominato Data Protection Officer ed ha accettato l'incarico, così come definito nel GDPR.

La Casa di Cura ha inoltre provveduto alla nomina di amministratori di sistemi esterni in relazione ai corrispondenti incarichi affidati in outsourcing.

3.2. Compiti assegnati al responsabile della privacy e agli incaricati. La gestione degli interessati.

3.2.1. La nomina ed il ruolo del Responsabile

Il Responsabile della Privacy della DL ha il compito, in nome e per conto del Titolare, di nominare formalmente eventuali altri Responsabili con specifiche lettere di incarico che avrà cura di conservare controfirmate per accettazione.

Ciascun Responsabile a sua volta può:

- nominare gli Incaricati del trattamento per le Banche di dati che gli sono state affidate;
- sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice;
- dare le istruzioni adeguate agli Incaricati del trattamento dei dati effettuato con strumenti elettronici e non;
- periodicamente, almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli Incaricati;
- chiedere la revisione dei profili di accesso se ritiene opportuna un eventuale restrizione.

Il Responsabile dovrà assicurare che si osservino le regole istituite:

- acquisire solo i dati necessari per le finalità dell'azienda;
- provvedere a raccogliere e a registrare dati, agli esclusivi fini dell'inserimento nelle banche dati e/o dell'arricchimento delle stesse, nei limiti e con le modalità e finalità previste nel registro dei trattamenti;
- curare l'esattezza ed il tempestivo aggiornamento dei dati;
- esercitare la dovuta diligenza affinché non vengano conservati dati non necessari o superflui;
- avere cura, secondo le comuni regole della prudenza e della diligenza, di trattare i dati stessi con la massima riservatezza e di impedire, per quanto possibile che estranei non autorizzati prendano conoscenza dei dati;
- restringere i profili di accesso al minimo indispensabile in relazione alle funzioni svolte;
- provvedere alla cancellazione dei dati nel momento in cui non ne sia più prevista la conservazione.

3.2.2. La nomina ed i ruoli degli Incaricati

Gli Incaricati al trattamento sono formalmente nominati dal Responsabile con una specifica lettera di incarico controfirmata. Le lettere sono tutte in corso di rinnovo in relazione alle nuove disposizioni previste dal GDPR.
Il Responsabile del trattamento avrà cura di conservare tali lettere controfirmate per accettazione.
In tali lettere sono dettagliati i principi cui l'incaricato deve attenersi per il trattamento dei dati personali, come definito al precedente paragrafo.

L'incaricato si assicurerà sistematicamente che, in caso di allontanamento dal posto di lavoro, i contenitori degli archivi e banche dati (scrivanie, cassetti, armadi, computer, ecc.) siano chiusi a chiave e/o protetti da password e che i dati dagli stessi estratti non possano divenire oggetto di trattamento improprio. In caso di sostituzione del computer utilizzato, si assicurerà che siano compiute le operazioni di formattazione dell'hard-disk, in maniera tale da rendere irrecuperabili i dati ivi contenuti.

Per garantire la piena funzionalità del trattamento dei dati anche in caso di mancanza di uno degli Incaricati, il Responsabile del trattamento dovrà provvedere ad addestrare e ad assegnare i diritti d'accesso di un determinato trattamento a più Incaricati.

L'elenco degli Incaricati al trattamento, con relative lettere controfirmate dagli interessati per accettazione, è custodito dal Responsabile del Trattamento ed aggiornato periodicamente.

3.2.3. L'acquisizione del consenso degli interessati

Nel caso di trattamento di dati sensibili, viene richiesto il consenso scritto dell'Interessato. Il consenso e l'Informativa sono stati revisionati per adeguarli a tutto quanto previsto nel GDPR. Nei casi previsti di maggior tutela per l'utente, si ritiene opportuno l'oscuramento dei dati in ogni caso, su richiesta del paziente.

Viene richiesto anche il consenso dell'interessato, come stabilito dalla normativa, al momento del ricovero, per determinare se l'interessato vuole o meno che venga comunicata agli eventuali visitatori la sua presenza in Casa di Cura. La procedura di acquisizione è dettagliatamente descritta nei documenti del Sistema di Gestione Qualità. Nel medesimo consenso è inoltre acquisita l'autorizzazione e fornire informazioni sullo stato di salute del degente solo ed esclusivamente ai familiari/autorizzati specificamente definiti dall'interessato.

E' compito di ogni Incaricato del trattamento e/o del Responsabile archiviare i documenti comprovanti il consenso dell'Interessato.
E' prevista nel prossimo biennio l'implementazione del sistema di acquisizione anche con firma grafometrica. La conservazione dei consensi in tal caso potrà avvenire digitalmente

3.2.4. La gestione dei diritti dell'interessato

La DL è opportunamente organizzata per poter far fronte alle richieste dell'Interessato, che in particolare ha il diritto:

- di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati,
- di ottenere la loro comunicazione in forma intelligibile;
- di ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del Titolare, e dei Responsabili;
- di ottenere l'indicazione dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;
- di ottenere l'aggiornamento, la rettifica e l'integrazione dei dati;
- di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- di stabilire se la Casa di Cura può comunicare, o meno, ad eventuali visitatori, la sua presenza in casa di Cura;
- di indicare chi può ricevere informazioni sul suo stato di salute;
- di conoscere quali sanitari hanno accesso ai dati contenuti nell'eventuale DSE;
- di richiedere l'oscuramento di tutti i suoi dati contenuti nel sistema (Diritto di oscuramento). In tal caso il paziente sarà cancellato dal Sistema Dedalus e tutta la documentazione sanitaria verrà conservata in un fascicolo cartaceo conservato dal Titolare del Trattamento, consultabile solo ed esclusivamente da chi registra data, ora nominativo e motivo della consultazione. Tale trattamento è in ogni caso riservato ai soggetti aventi diritto alla maggior tutela, in caso di richiesta.

Il responsabile del trattamento o il responsabile della privacy sono tenuti a verificare ed a controllare che l'incaricato soddisfi in tempi brevi e correttamente le richieste dell'interessato.

I dati estratti possono essere comunicati al richiedente verbalmente, ma di norma, se tecnicamente possibile e semplice, è opportuno fornire per iscritto, facendosi controfirmare una copia con data.

In caso di minori (con consenso già prestato da un genitore), divenuti maggiorenni, il sistema propone ulteriormente ed automaticamente l'acquisizione del Consenso.

4. Analisi dei rischi

L'analisi dei rischi è stata condotta con riguardo alle circostanze possibili o probabili che potrebbero determinare il verificarsi di vulnerabilità dei sistemi informativi con grave pericolo di distruzione o perdita dei dati, anche laddove accidentalmente procurata, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

L'analisi delle vulnerabilità del Sistema Informativo di DL ha contribuito alla rilevazione dei rischi che l'azienda stessa si potrebbe trovare a fronteggiare laddove si verificassero talune minacce sulla raccolta e conservazione dei dati, considerando che la Società occupandosi di Prestazioni Sanitarie è chiamata a trattare dati ascrivibili, ai fini della privacy, alla categoria dei dati sensibili.

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

1. rischi ambientali e fisici;
2. rischi relativi all'integrità dei dati;
3. rischi relativi alla riservatezza dei dati;
4. rischi relativi ai trattamenti non consentiti o non conformi alle finalità della raccolta;
5. rischi relativi alla continuità e disponibilità dei dati.

4.1. Rischi ambientali e fisici

Nella categoria dei rischi specifici sono stati compresi, classificati ed esaminati, tutti i rischi che, generalmente, non trovano una valida protezione nei sistemi di difesa adottati.

In particolare, sono considerati rischi quelli inerenti all'ubicazione dei luoghi in cui vengono custoditi i dati e svolte le diverse operazioni di trattamento, quelli inerenti i rischi idrogeologici, elettrici e di accesso fisico a infrastrutture, strumenti elettronici e impianti ausiliari.

Le infrastrutture fisiche ed elettriche sono dislocate nella sede della Società: ed in particolare, nei locali di Accettazione amministrativa e accettazione sanitaria (primo soccorso), nei locali adibiti al servizio amministrativo ubicati al 4° piano ed al piano terra, nelle Medicherie dei piani di degenza, negli Ambulatori medici, nel Laboratorio Analisi, nella Radiologia, nella sede distaccata del Servizio di fisioterapia, nel locale archivio e nel locale adibito al server (dotato di sistemi attivi e passivi antincendio, nonché registrazione degli accessi).

Le Cartelle Cliniche, dopo circa 12 mesi dalla chiusura vengono ritirate dalla CSP s.r.l. per essere custodite, archiviate, scannerizzate e messe a disposizione della Casa di Cura su un server con accessi controllati, tutto come descritto nel DPPS della CSP s.r.l.

Il rischio di discontinuità elettrica è attenuato dalla protezione con gruppi di continuità statici, dei quali è prevista la progressiva sostituzione in caso di usura per anzianità.

4.2. Rischi connessi alla protezione di aree e locali

In particolare, sono considerati rischi quelli inerenti accesso fisico a infrastrutture, strumenti elettronici e impianti ausiliari.

I rischi sono connessi al fatto che i server (dati sistema Dedalus, Argos e immagini radiologiche) sono ubicati in un locale non sorvegliato e che le Cartelle Cliniche, in una prima fase, sono custodite in un locale non sorvegliato e poi devono essere trasferite con trasporto su ruote.

Attualmente il rischio di accesso è mitigato dal fatto che:

- entrambi i locali sono sempre chiusi a chiave e la chiave è custodita esclusivamente dal Responsabile della Privacy o da incaricati del trattamento, all'uopo delegati.
- è stato inoltre istituito un registro degli accessi alla sala server che deve essere compilato da chiunque, ad accezione del responsabile informatico (UL), vi acceda per qualsiasi motivo.
- per quanto concerne il salvataggio dei dati dei sistemi Hospital e Argos, questo avviene su una NAS. Inoltre per le immagini radiologiche viene conservata una doppia copia dei dati di back up in luoghi separati.
- Vedi anche DPPS CSP.

4.3. Rischi relativi all'integrità dei dati

Il concetto di "integrità" riguarda la correttezza, la completezza e la consistenza dei dati sia con riferimento alla protezione dei medesimi, sia alla protezione dai rischi di alterazione o distruzione accidentali o dolose.

Detti rischi sono stati classificati in:

1) rischi connessi a fatti accidentali;
2) rischi derivanti da programmi di cui all'art. 615 quinquies del codice penale;
3) rischi connessi a fatti dolosi.

I rischi di intrusione, che possono provocare danni di integrità oltre che di riservatezza e disponibilità, sono rappresentati dalla possibilità che un soggetto interno (casistica più diffusa) od esterno all'azienda acceda a dati o sistemi, per scopi non leciti, violando la riservatezza, l'integrità o la disponibilità di dati o sistemi.

4.3.1. Integrità dei dati - Rischi connessi a fatti accidentali

Si tratta di rischi di alterazione o distruzione di dati che conseguono all'involontaria sovrascrittura imputabile ad azioni umane errate oppure a guasti delle apparecchiature dedicate alla memorizzazione.

In particolare, vi rientrano le alterazioni o distruzioni di dati dovute a:

- comandi applicativi o operativi errati
- malfunzionamenti hardware;
- deterioramento, nel tempo, dei supporti di memorizzazione e del mezzo fisico che li ospita;
- software pericoloso, in particolare a virus e tool sistemistici generalizzati

4.3.2. Integrità dei dati - Rischi da programmi pericolosi

I seguenti rischi sono connaturati alla diffusione di virus e di programmi pericolosi:

- corruzione dei file eseguibili e, a volte, dei dati;
- corruzione di documenti;
- perdita di file;
- perdita di spazio utilizzabile nelle memorie;
- cattivo funzionamento del sistema;
- degrado delle prestazioni del sistema;
- impossibilità di utilizzo del sistema;
- violazioni relative alle ipotesi di cui all'art. 615 quinquies del codice penale;
- danni alla reputazione dell'azienda.

Sulla base dell'analisi delle casistiche nazionali ed internazionali è possibile individuare i seguenti fattori distintivi delle attuali maggiori criticità riscontrate:

- diffusione di virus e worm che sfruttano vulnerabilità note dei programmi e dei sistemi più diffusi per introdursi nel Sistema Informativo;
- posta elettronica ed Internet utilizzati dagli autori di virus per diffondere codici dannosi e pericolosi (virus, cavalli di Troia, worm e backdoor);
- aumento di e-worm finalizzati ad attacchi DDOS (Distribuited Denial Of Service) contro siti scelti come obiettivo, ovvero lanciati a caso sulla rete;

In sintesi, i virus ed i programmi pericolosi si diffondono principalmente attraverso:

- Internet, mediante la posta elettronica;
- Internet, attraverso la semplice connessione a siti infetti o attraverso il prelievo di file corrotti;
- supporti removibili, ed in particolare CD Rom, pen drive e USB infetti provenienti da terzi o importati dai dipendenti senza l'autorizzazione dell'azienda;

Per mitigare i rischi connessi alla diffusione di virus o di programmi pericolosi la DL utilizza sui nuovi pc antivirus built-in Windows Defender. Altri hanno prodotti diversi (Avira, Kasperski, Avast, ecc) con licenze diverse per ogni postazione. I sistemi antivirus costantemente aggiornati. **Il server (multilicenza) protetto da un firewall costantemente aggiornato, per la protezione rispetto ad intrusioni esterne, per il quale è comunque in coro di predisposizione una revisione di tutto il sistema di protezione al fine di renderlo ancora più efficace.**

Il sistema antivirus esegue il controllo di ogni e-mail in ingresso ed in uscita per la protezione dei server di posta elettronica e conseguentemente dei client che al server si collegano con accessi controllati tramite Server proxy (in corso di revisione). Vi è inoltre un dominio dilorenzo.it un servizio antivirus ed antispam per le caselle di posta elettronica.

Il rischio di integrità dei dati è connesso alla possibilità da parte degli utenti di configurare una connessione remota ad internet sui PC portatili, e conseguentemente di collegarsi al di fuori delle misure di sicurezza adottate, esponendo la DL al rischio che vengano introdotti programmi malevoli sui portatili durante queste connessioni non protette e successivamente nel sistema della casa di cura**.**

Tutti i dati contenuti su PC contenenti dati riservati vengono periodicamente sottoposti al back up dei dati come programmato, su hard disk esterno, conservato presso la Direzione Amministrativa. Non è consentita l'introduzione ed il collegamento di PC non gestiti dal Sistema Informatico della casa di Cura.

Tutti i dati del sistema Dedalus e Argos nonchè delle immagini radiologiche sono gestiti ed archiviati su server separati ed in copia su dischi. Per questo tipo di dati (non ambiente windows) è fortemente ridotto il rischio di contrarre i virus diffuramite web.

La Casa di Cura nell'anno 2017 ha commissionato alla Project Innovation uno studio su tutta l'infrastruttura informatica della Società per verificare l'aggiornamento dei sistemi di protezione e l'efficacia delle misure di sicurezza, nonché l'aggiornamento dell'intero parco Hardware. Dall'analisi sono emerse criticità classificate in differenti gradi di pericolo ed è stato quindi avviato un programma di investimenti per la risoluzione a breve termine delle criticità maggiori, nonché di programmazione per la risoluzione delle criticità minori o differibili. Il report dell'attività effettuata è conservato dal Titolare del trattamento. (vedi allegata analisi dei rischi).

Un ulteriore livello di sicurezza è dato dall'istituzione del server di Dominio, mediante il quale la singola utenza di sistema non possiede i privilegi di apportare modifiche ai sw installati sul sistema, né di installare nuovi software. Questo inibisce l'installazione di applicazioni a carattere malevole sui terminali degli utenti.

4.3.3. Integrità dei dati - Rischi connessi a fatti dolosi

Sono comprese tutte le alterazioni dell'integrità dei dati conseguenti ad azioni dolose perpetrate allo scopo di:

- modificare i dati;
- inserire nuovi dati;
- distruggere i dati.

4.4. Rischi di Riservatezza dei dati, e Rischi di trattamenti non consentiti o non conformi alle finalità della raccolta

Tale rischio è stato esaminato in relazione alla possibilità che si realizzino rilasci di informazioni non autorizzati e/o accessi non autorizzati ai dati.

Per quanto attiene la "riservatezza" si è fatto in modo di garantire la dovuta protezione delle informazioni contro ipotetiche divulgazioni non autorizzate, consentendo l'utilizzo ed il trattamento solamente ai soggetti incaricati dei trattamenti.

Sono stati valutati i seguenti rischi:

1) rischi di accessi fraudolenti dall'interno:

   tali rischi sono dovuti a:
   - un "profilo" di autorizzazione all'accesso non aderente al ruolo assegnato o conseguente all'attribuzione di "privilegi" di accesso eccessivi.
   - "inferenza", ossia alla cattura di informazioni che, se correlate, consentono di giungere alla conoscenza indiretta di dati.
   - utilizzo dei privilegi di "amministratori di sistema" per l'accesso ad archivi.
   - "personificazione" di un soggetto autorizzato all'accesso ai sistemi.
   - "manomissione" delle autorizzazioni da parte del personale addetto al controllo ed all'amministrazione dei profili di accesso.

Tali rischi sono eliminati dalla non condivisione delle stazioni di lavoro se non con specifica autorizzazione dell'amministratore dei sistemi che opera sotto la supervisione del legale rappresentante della società, grazie all'attribuzione di password per l'accesso ad alcune postazioni contenenti dati riservati ed inoltre grazie ai profili di accesso per singolo utente che non consentono l'accesso ad aree riservate del sistema. Il profilo di accesso, definito per gruppi, viene associato al soggetto al momento della prima assegnazione di password e ne è stata recentemente effettuata un'attenta revisione con restrizione dei profili di accesso.

4.5. Rischi di Continuità e Non Disponibilità dei dati

Il concetto di "disponibilità" dei dati è riferito alla necessità di assicurare che l'accesso ai dati sia sempre disponibile, evitando la perdita o la riduzione dei sistemi, dei dati e dei servizi.

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

4.5.1. Non Disponibilità - Rischi di carattere accidentale

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

- anomalie in programmi
- errori commessi dal personale
- malfunzionamento dell'hardware
- dimensionamento non sufficiente delle risorse tecnologiche
- non continuità del servizio

I rischi di carattere accidentale sono mitigati da interventi tempestivi della ditta responsabile della manutenzione degli strumenti informatici "Project Innovation srl", con il supporto del responsabile Domenico Canerossi, nonché della Dedalus s.p.a. per gli interventi, anche da remoto, sui software forniti. Inoltre, la recente sostituzione del server, tecnologicamente superiore, consente un recupero e ripristino pressoché immediato dei dati.

Le immagini radiologiche vengono rese immediatamente disponibili su CD separati ed in ogni caso rimangono nella memoria (prima dell'apparecchio radiologico e poi del server) qualora vi siano guasti che non consentono l'archiviazione su CD dovuta a malfunzionamenti del masterizzatore. In caso di necessità di visualizzazione immediata delle immagini, le stesse vengono stampate su pellicola anziché visualizzate a video (se guasto) e masterizzate su CD (se guasto).

4.5.2. Non Disponibilità – Rischi di carattere intenzionale

In questa tipologia di rischi sono incluse le fattispecie in cui le informazioni non sono disponibili a causa di azioni umane volontarie, compiute con lo scopo preciso e determinato di impedire l'accesso alle informazioni da parte di soggetti autorizzati.

Tali minacce sono messe in relazione a danneggiamento o manomissione di sistemi per infedeltà del personale addetto alla gestione delle informazioni.

I rischi intrinseci sono mitigati da controlli organizzativi e la supervisione del responsabile al trattamento dei dati, nonché dalle procedure di gestione dei documenti previste dal Sistema di Gestione Qualità certificato e dal sistema di selezione, addestramento e valutazione del personale che viene assunto in Casa di Cura.

4.6. Data Breach

In ogni caso, qualora si dovesse verificare, per qualsiasi ragione, una violazione dei dati, il Data Protection Officer Dott. Gabriele Pizzi Scatena, in collaborazione con il Titolare del Trattamento, Dott.ssa Lucia Di Lorenzo, provvede entro 48 ore lavorative alla Comunicazione al garante, come previsto nel relativo regolamento, con la modulistica prescritta dal Garante ed informa altresì l'interessato cui si riferisce l'eventuale violazione.

E' in corso di integrazione la PO-UL-INF per definire le modalità operative di gestione del data breach.

5. Misure organizzative per garantire la protezione dei dati

Sono state emanate e tenute aggiornate specifiche policy sulla segretezza delle password per tutto il personale.

Il personale è stato sensibilizzato sulle problematiche di rischio inerenti le credenziali di autenticazione ed i sistemi di posta elettronica.

L'attività formativa sul tema viene rinnovata con cadenza biennale, l'ultimo evento formativo si è svolto tra l'anno 2015 e l'anno 2016. Sono già programmati eventi formativi per il biennio 2018-2019 (vedi piano di formazione).

6. Misure da adottare per garantire la protezione delle aree, dei locali e degli impianti

6.1. Protezione delle aree e dei locali

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.

Gli uffici sono protetti da porte chiuse a chiave.

Il personale di segreteria verifica gli accessi in entrata.

I dati personali contenuti nei documenti cartacei sono custoditi in un apposito archivio sotto il controllo del personale addetto alla segreteria ed autorizzato ad accedervi.

In particolare, la sala server è dotata di impianto rileva fumi e porta antincendio. Tale porta risulta chiusa a chiave e gli accessi sono controllati mediante specifico registro.
Le chiavi sono in possesso dell'Amministratore di Sistema sig. Domenico Canerossi, della Project Innovation ed il Responsabile del trattamento Sig.ra Patrizia Iacoboni ne conserva una copia.
E' stata istallata l'unica telecamera a circuito chiuso presente in Casa di Cura (area non aperta al pubblico), all'esterno della sala server puntata sulla porta d'ingresso, opportunamente segnalata per consentire l'identificazione di eventuali responsabili di intrusioni con finalità illecite. Vi è inoltre uno specifico segnalatore di fumo all'interno della sala server.

7. Misure di sicurezza per garantire l'integrità e disponibilità dei dati

Le tecniche ed i sistemi di sicurezza adottati dalla DL per la protezione dei dati personali e sensibili fanno riferimento sia al trattamento informatico che non.

Le misure di sicurezza adottate risultano idonee alla protezione dei dati e soddisfano le misure minime richieste dal Codice della Privacy e l'esigenza di un adeguato livello di protezione dei dati.

7.1. Misure di sicurezza per la prevenzione dei rischi di carattere accidentale

Al fine di garantire il ripristino dei dati è previsto il salvataggio dei dati con frequenza giornaliera.

É in vigore una procedura per l'effettuazione dei back up al fine di realizzare gli obiettivi temporali di ripristino.

Sono di seguito identificati gli interventi a carico di DL:

- Il contenuto dei PC in locale sarà progressivamente (in corso di censimento e predisposizione dell'attività) automaticamente salvato sul server con cadenza definita e in base al censimento effettuato e registrato
- I dati sui server sono salvati settimananlmente con unità di back up automatico.
- I dischi che contengono i back up sono custoditi in luoghi separati dal server.
- Nel processo di sensibilizzazione e formazione del personale, viene costantemente dedicata particolare attenzione, anche tramite note informative, sulla necessità di attuare comportamenti conformi alle corrette procedure di gestione delle informazioni trattate in modalità elettronica, al fine di garantirne l'integrità e la disponibilità nel tempo.
- Per minimizzare eventuali problemi dovuti a guasti hardware si provvede ad una costante manutenzione degli apparecchi e alla copertura dei rischi con garanzia del produttore/fornitore.
- Tutti i PC con sistema operativo obsoleto e non in grado di supportare i sistemi operativi più recenti, in grado di garantire la sicurezza, sono in corso di sostituzione e sugli stessi sono istallati sistemi operativi ed antivirus recenti, ferma restando la barriera costituita dal firewall centralizzato.

7.2. Aggiornamenti periodici dei programmi per elaboratore volti a prevenire le vulnerabilità degli strumenti elettronici (patching software)

Gli aggiornamenti periodici alle versioni di software sui singoli PC consentono di eliminare delle vulnerabilità intrinseche di questi software al momento del loro rilascio da parte del fornitore.

Questi aggiornamenti vengono chiamati patch (effettuati durante la normale operatività) oppure Hot fix (in caso di grave vulnerabilità da rimuovere con urgenza nel corso di attacchi).

Le macchine di nuova o ultima istallazione hanno sistemi operativi Windows recenti, in grado di garantire sicurezza contro le intrusioni.

Gli aggiornamenti di configurazione dei software sulle singole postazioni di lavoro e sui server vengono effettuati in modo tempestivo anche con l'utilizzo di autoupdate di Microsoft; tali interventi sono affidati alla Project Innovation. I singoli utilizzatori di PC sono comunque istruiti sulla necessità di procedere agli aggiornamenti.

7.3. Sicurezza delle trasmissioni dei dati

L'accesso ad Internet avviene transitando dal firewall, in modo tale da avere garanzie sui filtri di sicurezza impostati.

In aggiunta è in corso di rinnovo nel proxy una "black list" dei siti sui quali non è possibile navigare, che sarà aggiornata con periodicità almeno annuale (salvo ulteriori richieste). Alcuni PC, con eccessivo numero di utilizzatori non hanno alcun accesso ad internet, nemmeno se l'utilizzatore è fornito di PW per il proxy. Infine, nel caso di utilizzo di IP dinamici (tramite rete wireless), gli accessi sono comunque registrati. Degli IP dinamici 3 sono bloccati ad uso delle postazioni Argos di reparto. Attraverso gli IP dinamici non è possibile ricevere posta elettronica. **Al momento non tutti i pc, per via del firewall, si aggiornano. E' stato bypassato il problema installando all'interno dell'azienda un sistema WSUS (Windows Server Update Services – servizio di aggiornamento per sistemi operativi Microsoft Windows) che è in corso di tuning post installazione.**

E' stato istallato un captive portal per l'accesso dei pazienti alla rete wireless, su rete differente, con altro server e accesso con password a scadenza, che viene assegnata al momento del ricovero, su richiesta dell'interessato per il numero di giorni previsti di degenza, con scadenza automatica.

Per quanto concerne l'invio dei referti e delle copie delle Cartelle Cliniche (in formato .pdf) su richiesta dei pazienti, attualmente, non disponendo di un apposito programma di cifratira referti, l'invio può essere effettuato, solo su richiesta dell'interessato ricevuta via PEC o controfirmata in originale dal paziente stesso, attraverso la PEC stessa della Casa di Cura. Eventuali ulteriori azioni di implementazione e miglioramento saranno realizzate in occasione dell'attivazione della sezione di consultazione dei referti on line sul sito internet della Casa di Cura nella realizzazione del quale si terrà conto di tutte le indicazioni di sicurezza richieste dal Garante e dell'eventuale rilascio di consenso nel caso di utilizzo dei cookies.

7.4. Misure di sicurezza contro il rischio di intrusione

I rischi di intrusione sono rappresentati dalla possibilità che un soggetto interno (casistica più diffusa) od esterno all'azienda acceda a dati o sistemi, per scopi non leciti, violando la riservatezza, l'integrità o la disponibilità di dati o sistemi.

Detta condotta può essere realizzata anche attraverso l'uso di programmi malevoli.

Le contromisure contro i rischi esterni di intrusione sono prevalentemente architetturali (firewall fisici, configurazioni non standard, eliminazione di porte logiche inutili) o legati alla dotazione di software all in one (antivirus, antispyware, antispam, antipishing, parental control e firewall software in un unico prodotto) che forniscono una protezione dalle minacce di Internet a più livelli.

I sistemi antintrusione consistono in:

- i firewalls sono configurati secondo i criteri di tutte le connessione in entrata negate e tutte le interconnessioni in uscita abilitate.

Una contromisura efficace è rappresentata dalla registrazione dei log delle attività dei sistemi in tutti i punti critici del sistema.

I software di protezione sono le contromisure consigliate contro i programmi malevoli. Essi consentono inoltre di individuare i programmi potenzialmente dannosi già presenti nei singoli sistemi ed intervengono bloccandone il funzionamento.

È fatto divieto di utilizzare software non ufficialmente rilasciato.

Nel caso in cui si verifichi una contaminazione da virus è prevista una procedura di intervento immediato di isolamento del PC al fine di minimizzare la diffusione del virus e l'impatto sull'azienda; successivamente, si analizzano le cause del problema per eliminarle e ripristinare il normale funzionamento del PC.

E' stato effettuato il monitoraggio della efficacia della diffusione degli ultimi aggiornamenti distribuiti sull'intero parco macchine.

7.5. Misure di autenticazione informatica ed autorizzazione per l'accesso ai dati del software Dedalus e dominio

Di seguito vengono descritti i criteri e le procedure adottati per garantire la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica.

7.5.1. Misure per il controllo dell'accesso Sistema di autenticazione

Per la connessione alla rete interna è prevista una procedura di autenticazione mediante il codice identificativo dell'utente e la relativa password.

Sono state fornite a tutti i dipendenti le indicazioni per l'elaborazione delle password: devono avere 8 caratteri alfanumerici contenenti anche simboli ed essere facilmente memorizzabili per l'utente.

Le password di accesso sono scelte dall'utente in totale riservatezza e il Sig. Domenico Canerossi assegna, contestualmente, i profili di utilizzo e registra l'avvenuta assegnazione delle password di accesso.

Le password di accesso con i relativi profili sono archiviate nel sistema, ma non visibili; l'elenco degli utenti con password assegnata è costantemente aggiornato dal sistema e riproducibile su carta.

7.5.2. Autonoma sostituzione della parola chiave

È prevista l'autonoma sostituzione della parola chiave ogni 90 giorni o ogniqualvolta l'utente lo considerasse necessario.

Tramite interventi di formazione/sensibilizzazione è stato comunicato ai dipendenti che la parola chiave può essere utilizzata anche per proteggere singoli file elettronici o cartelle contenenti dati riservati, ma il personale non è comunque autorizzato a detenere dati personali e riservati sui PC della DL.

E' possibile il collegamento alla rete WI FI dedicata alla gestione Argos (cartella clinica informatizzata) solo ed esclusivamente ai PC portatili per la visita in reparto con sistema Argos, custoditi nelle medicherie in armadio chiuso a chiave. La Password per l'accesso alla rete WI FI è conservata, come le altre, dal Responsabile del Trattamento e dal Responsabile Informatico.

7.5.3. Soggetti preposti alla custodia delle credenziali di autenticazione

È operativo un sistema (super user) che assicura la disponibilità di dati o strumenti elettronici tramite parola chiave in caso di prolungata assenza o impedimento da parte dell'utente incaricato o in caso di definitiva cessazione del rapporto. Dopo la cessazione del rapporto o in caso di prolungata assenza la password viene comunque disabilitata, ma rimane in memoria nel sistema chi ne è stato l'utilizzatore ed il relativo periodo. La gestione di questi sistema è delegata al custode delle password (Domenico Canerossi).

E’ stato istallato un sistema di refertazione da remoto per la sola radiologia. Viene effettuato accesso dal radiologo autorizzato (da un suo PC protetto da PW) su una VPN dedicata che verifica il certificato digitale personale.

Inoltre la CSP si collega attualmente attraverso la rete della Casa di Cura, ma si sta valutando la possibilità di garantire una VPN dedicata. In ogni caso i rischi sono irrilevanti poiché la CSP è dotata di un proprio DPPS ed è comunque autorizzata al trattamento dei dati sensibili dei pazienti (in quanto gestisce le Cartelle Cliniche).

7.5.4. Istruzioni non accessibilità strumento elettronico

Si stanno progressivamente dotando le macchine, per le quali se ne rilevi la necessità, di blocco con password in caso di temporanea assenza dell’utente.

7.6. Misure per la gestione delle autorizzazioni

7.6.1. Autorizzazione all’accesso agli strumenti

Tutti gli strumenti dai quali si può accedere ai dati sono censiti e codificati.

È operativo un sistema informativo ed informatico nel quale le autorizzazioni non si riferiscono mai a tali strumenti bensì ai singoli operatori.

È attivo un sistema di log che consente di risalire ai dati relativi al sistema e all’operatore che hanno eseguito una specifica operazione.

L’accesso alla rete Dedalus, che prima avveniva con password, ma senza identificazione dell’utente sulla singola operazione, è adesso possibile solo con indicazione dell’utente (cui è stato attribuito un numero di accesso) per le operazioni amministrative. E’ in corso di implementazione da parte della Dedalus un sistema di registrazione dei log di accesso che consenta l’adesione completa a quanto previsto dalle regole per la gestione del DSE.

7.6.2. Autorizzazioni agli incaricati del trattamento

Con riguardo alle autorizzazioni è attiva una politica aziendale che persegue la logica del “minimo privilegio”, per cui le autorizzazioni sono legate al reale bisogno di accesso ai dati (*need to know e need to do*) da parte del personale della DL nell’espletamento delle mansioni lavorative assegnate, tramite un sistema di profili.

Tutte le autorizzazioni verranno sottoposte a verifica periodica (almeno annuale) in relazione alla permanenza delle necessità di accesso.

7.6.3. Misure per il controllo dell’accesso ai dati in locale su PC

L’accesso ai dati di carattere personale all'interno delle risorse del singolo personal computer è regolato da parola chiave per i PC per i quali l’amministrazione ne ha ravvisato la necessità. **E’ in corso l’installazione del dominio e l’inserimento dei pc aziendali all’interno di questo; così facendo ogni utente, per accedere ai pc, dovrà utilizzare le proprie credenziali che hanno le stesse politiche di sicurezza dei software della clinica (scadenza password a 90 giorni, utilizzo di caratteri alfanumerici maiuscoli/minuscoli, etc)**

Le persone autorizzate al trattamento dei dati personali vengono identificate a priori con lettera di incarico controfirmata per accettazione ed il loro accesso è regolato dalla stesura di particolari profili di autorizzazione distinti per tipologia di trattamento effettuato.

7.7. Misure atte a garantire la disponibilità di dati e sistemi

7.7.1. Postazioni di lavoro – Hardware di rete

Il rischio di non disponibilità dei singoli PC degli utenti è presidiato mediante un contratto di manutenzione con società terze che prevede l'assistenza in loco e la sostituzione tempestiva dei PC eventualmente non riparabili. Inoltre il responsabile delle copie di sicurezza ha sempre un PC ed una stampante con tutti i parametri per l'accesso alla rete, già configurato, per la sostituzione immediata e temporanea.

Il ripristino dei dati delle singoli stazioni di lavoro per i dati considerati rilevanti per la banca sono ripristinati dal file server appena sostituito il PC.

7.7.2. Ripristino in tempi certi

Il ripristino di tutti i sistemi è garantito in 24 ore lavorative.

In caso di pronto intervento da parte di Fornitori esterni, viene richiesta, rilasciata ed archiviata una attestazione degli interventi tecnici effettuati sui sistemi di sicurezza e relativamente al ripristino dei dati.

7.7.3. Registro eventi anomali

La registrazione degli eventi anomali viene effettuata attraverso il Sistema di Gestione Qualità con l'apertura di una Non Conformità, annotando anche le caratteristiche del virus o altro evento anomalo, la sua origine, gli effetti provocati e la risoluzione del problema. Nel caso di violazioni di particolare gravità si attiva la segnalazione del Data Breach come previsto al par. 4.6.

7.7.4. Continuità elettrica

Tutta la sala server è posta sotto continuità elettrica grazie ad UPS.

7.8. Ulteriori misure per la riservatezza disponibilità e integrità dei dati

7.8.1. Policy e regolamenti

È organicamente integrato nelle Procedure Operative del Sistema Gestione Qualità, il regolamento relativo alle misure per la protezione dei dati personali, tramite costante aggiornamento, con revisioni delle relative PO. In particolare, tale regolamento è inserito nella Procedura Operativa "Cartella Clinica" e nelle procedure di Gestione dei Servizi e della Contabilità Clienti.

È stato altresì adottato un Regolamento relativo all'utilizzo degli strumenti informatici, tramite l'emanazione della Procedura Operativa "Gestione Informatica e privacy" integrato nel SGQ, contenente anche le prescrizioni inerenti l'uso corretto di internet e della posta elettronica, nonché quelle relative alla dismissione/rottamazione dei pc.

Nella citata PO è inserito come allegato l'inventario dei client, delle stampanti, delle condivisioni, della possibilità di accesso alla rete e dei relativi IP.

Ulteriore strumento di controllo è l'audit interno annuale che viene effettuato, in base alla check-list allegata per verificare il rispetto di tutte le prescrizioni normative.

Il questionario di Costomer Satisfaction è aggiornato con la relativa informativa.

La Casa di Cura ha implementato un proprio ***Modello di Organizzazione, Gestione e Controllo per la responsabilità amministrativa***, conforme ai requisiti individuati nel **D.Lgs. 231/2001** e pertanto, ha effettuato:

- Nomina dell'Organismo di Vigilanza e Controllo (OdV) ed emanato relativo regolamento di funzionamento dell'Organismo stesso;
- Elaborato e distribuito a tutti il Modello Organizzativo (Parte Gen. + parti Spec.) e il "Codice Etico";
- Mappato tutte le attività a rischio reato e definito i processi sensibili da analizzare (Analisi del rischio), per i quali ha emanato/revisionato le apposite procedure;
- Definito Mansionari, Deleghe e Procure;
- Definito e condiviso un Sistema Disciplinare e Sanzionatorio – Sistema Premiante;
- Formazione del personale;
- Analizzato e monitorato attraverso audit interni condotti dall'ODV le attività identificate e definito i flussi informativi verso l'OdV.

7.8.2. Riutilizzo controllato dei supporti

I PC dismessi vengono catalogati e restituiti alla ditta fornitrice del sostituto oppure conservati presso un magazzino, previa cancellazione di tutti i dati in essi registrati.

Qualora i dati contenuti su determinati supporti non debbano più essere conservati e non sia possibile provvedere alla loro semplice cancellazione i supporti vengono distrutti.

8. Piano di formazione

Il piano di formazione è finalizzato a rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

Per tutto il personale incaricato del trattamento è stata effettuata nel 2015-2016, la formazione sui temi:

- informazioni sul D. Lgs. n. 196/03 e su disciplinare tecnico;
- rischi possibili e probabili cui sono sottoposti i dati;
- misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi;
- misure di sicurezza fisiche;
- misure di sicurezza organizzative;
- misure di sicurezza logiche;
- comportamenti e modalità di lavoro per prevenire i rischi, 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 anti-hacker), contenitori di sicurezza (ad es.: schedari, archivi, etc.), sistemi anti intrusione, importanza e modalità di realizzazione delle operazioni di backup, con particolare riguardo alle recenti novità introdotte dal Garante: amministratore di sistema, uso corretto del web (internet/email), dismissione/rottamazione dei pc, etc.;
- l'Ufficio del Garante;
- novità introdotte con il DSE e il Regolamento Europeo;

Ulteriori attività formative sono state eseguite ed in particolare: Gestione della Cartella Infermieristica e istruzioni di utilizzo cartella clinica informatizzata, miglioramento della sicurezza in relazione ad eventi di rischio clinico).
Nel 2018 è programmata la formazione specifica sull'entrata in vigore del GDPR e le novità dallo stesso introdotte.
Infine, la formazione in materia è sempre prevista al momento dell'assunzione nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti rilevanti rispetto al trattamento dei dati personali.

9. Trattamenti affidati all'esterno

Nella seguente tabella sono riportati i trattamenti affidati all'esterno:

Descrizione sintetica dell'attività esterna	Trattamenti di dati interessati	Soggetto esterno	Descrizione criteri/impegni
Sistema gestionale utenti	Pazienti	Dedalus	Nomina/contratto
Gestione Paghe e contributi	Personale	Studio Manerin	Nomina/contratto
Archiviazione Cartelle cliniche	Pazienti	CSP srl	Nomina/contratto
Gestione contabilità	Personale	Studio Giacobini	Nomina/contratto
Analisi di laboratorio ed esami istologici in service; breath test in service	Pazienti	Guidonia (ex ADI); Synlab (ex Fleming Labs); ditta qualificata di fornitura breath test	Nomina/contratto
Fornitura di tessuti	Pazienti	SSR Emilia Romagna	Nomina/contratto

10. Cifratura dei dati o separazione dei dati identificativi

Questa struttura sanitaria protegge tutti i dati personali sensibili idonei a rivelare lo stato di salute o la vita sessuale dei clienti utilizzando le modalità previste dal produttore del software soddisfacenti la normativa ed indicate nella tabella seguente:

Trattamento del dato	Protezione scelta	Data di effettività	Tecnica adottata	Informazioni utili
DB clienti-sistema Dedalus	Separazione tra dati identificativi e dati sensibili	2000	Gli archivi non sono criptati con tecniche di cifratura, ma sono illeggibili senza i corrispondenti tracciati di transcodifica (ODBC) in possesso solo di utenti autorizzati.	Il fornitore ha rilasciato dichiarazione formale sulla modalità della protezione scelta, che ne attesti la conformità alle disposizioni del disciplinare tecnico-allegato B al Dlgs 196/2003

11. Allegati

Sono parte integrante del presente DPPS i seguenti documenti:

1. PO-UL-INF (Gestione informatica e privacy)
2. IO-BUS (Back up server)
3. Modulistica
4. Check-list di verifica adempimenti privacy: ultimo aggiornamento
5. Verbale di controllo annuale: assegnazione profili di accesso; vigenza password; controllo IPA
6. Registro dei trattamenti del Titolare
7. Registro dei trattamenti del Responsabile

Avezzano, 24/7/2018

Il Titolare del Trattamento