Casa di Cura Privata 'Di Lorenzo' spa
Sede legale • via V. Veneto, 37 - 67051 Avezzano (Aq)
Ingresso utenti • via G. Amendola, 22
tel • 0863.4281 fax • 0863.412446 email • info@dilorenzo.it www.dilorenzo.it
PI/CF • 09037401008

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*:08/03/2024**

Approvato da: Lucia Di Lorenzo (Titolare del trattamento)

Relativo all'azienda: Casa di Cura Di Lorenzo spa (DL)

INDICE

Casa di Cura Privata 'Di Lorenzo' spa
Sede legale • via V. Veneto, 37 - 67051 Avezzano (Aq)
Ingresso utenti • via G. Amendola, 22
tel • 0863.4281 fax • 0863.412446 email • info@dilorenzo.it www.dilorenzo.it
PI/CF • 09037401008

Introduzione e Contesto

Il presente documento costituisce l'aggiornamento per l'anno 2024 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 ogni volta che ve ne sia l'opportunità; sia per accertare l'adeguamento normativo, sia per accertare il permanere di tutte le condizioni di sicurezza ivi previste.

Con l'adeguamento 2024, in particolare si è provveduto ad eliminare una serie di informazioni ritenute superflue in quanto già trattate in altra documentazione della Casa di Cura di Lorenzo.

Il presente documento è coordinato con il Registro dei trattamenti, in continuo aggiornamento, che ne costituisce parte integrante e sostanziale.

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

La struttura aziendale

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

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. Ogni nuovo incaricato sottoscrive la relativa documentazione.

Responsabili del trattamento dei dati personali

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. Ogni nuovo incaricato sottoscrive la relativa documentazione. I Responsabili privacy sono ad ogni modo identificabili nella documentazione inerente la privacy.

Designazione del Responsabile della Sicurezza

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, sono stati designati come sostituti per le funzioni attribuite il Dott. Maurizio Gentile e il Sig. Alessandro Lusi. Al Sig. Massimiliano Lupi è stato conferito l'incarico di amministratore di Sistema in qualità di Social Media Manager. E' stata inoltre incaricata della gestione dell'infrastruttura informatica della Società Di Lorenzo la Project Innovation s.r.l. Il Dott. Gabriele Pizzi Scatena è stato, infine, nominato Data Protection Officer.

Casa di Cura Privata 'Di Lorenzo' spa
Sede legale • via V. Veneto, 37 - 67051 Avezzano (Aq)
Ingresso utenti • via G. Amendola, 22
tel • 0863.4281 fax • 0863.412446 email • info@dilorenzo.it www.dilorenzo.it
PI/CF • 09037401008

Analisi dei Rischi

Legenda:

✔ - Misura implementata

🏗 - Misura in corso di implementazione

📅 – Misura pianificata o da pianificare

Accesso non autorizzato

Valutazione:

Rischio di accesso non autorizzato alle informazioni sanitarie da parte di personale non autorizzato.

Impatto:

Responsabilità legale: La violazione della sicurezza delle informazioni sanitarie potrebbe comportare azioni legali da parte dei pazienti colpiti. Queste azioni legali potrebbero portare a pesanti sanzioni finanziarie e danni all'immagine della casa di cura privata.

Perdita di reputazione: La divulgazione non autorizzata di informazioni sanitarie potrebbe danneggiare gravemente la reputazione della casa di cura privata. La cattiva pubblicità potrebbe influire sulla capacità di attirare nuovi pazienti e collaboratori, compromettendo la crescita e la sostenibilità finanziaria della struttura.

Misure:

Implementazione di controlli di accesso robusti: Impiegare sistemi di gestione degli accessi che permettano solo al personale autorizzato di accedere alle informazioni sanitarie. Questi sistemi sono basati su ruoli e limitare l'accesso solo alle informazioni pertinenti per ciascun membro del personale. ✔

Formazione del personale: Fornire formazione regolare al personale sulla sicurezza delle informazioni e sulla conformità alle normative sulla privacy. Creare una consapevolezza della responsabilità individuale nel mantenere la riservatezza delle informazioni sanitarie. ✔

Monitoraggio continuo: Implementare sistemi di monitoraggio che identifichino e registrino gli accessi non autorizzati alle informazioni sanitarie. Questo consentirà di individuare tempestivamente eventuali violazioni e intraprendere azioni correttive immediate. ✔

Aggiornamento delle politiche di sicurezza: Mantenere aggiornate le politiche e le procedure di sicurezza delle informazioni, garantendo la conformità con le normative vigenti e adottando le best practice del settore. ✔

Collaborazione con esperti in sicurezza informatica: Coinvolgere consulenti o esperti in sicurezza informatica per valutare e migliorare la robustezza del sistema di sicurezza delle informazioni, garantendo la protezione continua contro minacce interne ed esterne. ✔

Casa di Cura Privata 'Di Lorenzo' spa
Sede legale • via V. Veneto, 37 - 67051 Avezzano (Aq)
Ingresso utenti • via G. Amendola, 22
tel • 0863.4281 fax • 0863.412446 email • info@dilorenzo.it www.dilorenzo.it
PI/CF • 09037401008

Perdita o furto di dispositivi

Valutazione:

Rischio di perdita o furto di dispositivi contenenti dati sanitari, come laptop, tablet o dispositivi di memorizzazione.

Impatto:

Violazione della privacy dei pazienti: La perdita o il furto di dispositivi contenenti dati sanitari potrebbe portare a una compromissione della privacy dei pazienti, con potenziali conseguenze negative sulla fiducia dei pazienti e sulla reputazione della struttura sanitaria.

Possibile accesso non autorizzato: I dispositivi rubati o smarriti potrebbero essere utilizzati da persone non autorizzate per accedere ai dati sanitari sensibili, mettendo a rischio la sicurezza delle informazioni e la conformità alle normative sulla privacy.

Rischio di furto di identità: I dati sanitari possono essere utilizzati per attività fraudolente, inclusa la creazione di identità fittizie o l'accesso indebito a servizi sanitari, aumentando il rischio di furto di identità per i pazienti coinvolti.

Misure:

Crittografia dei dati: Implementare la crittografia per proteggere i dati sui dispositivi. In caso di perdita o furto, questa misura rende difficoltoso l'accesso ai dati senza le adeguate chiavi di decrittazione. 

Politiche di sicurezza dei dispositivi: Stabilire e far rispettare politiche di sicurezza rigorose per l'uso e la gestione dei dispositivi contenenti dati sanitari. Ciò può includere l'obbligo di utilizzare password complesse, la disattivazione di funzionalità non necessarie e la segnalazione immediata di perdite o furti. ✔

Monitoraggio remoto: Implementare soluzioni di monitoraggio remoto che consentano di localizzare e disabilitare i dispositivi smarriti o rubati. Queste soluzioni possono aiutare a ridurre il rischio di accesso non autorizzato ai dati. ✔

Backup regolari: Effettuare backup regolari dei dati su dispositivi mobili. In caso di perdita o furto, i dati possono essere rapidamente ripristinati, riducendo al minimo l'impatto sulla continuità operativa. 

Formazione del personale: Fornire formazione regolare al personale sull'importanza della sicurezza dei dispositivi e sulle procedure da seguire in caso di smarrimento o furto. La consapevolezza del personale è cruciale per prevenire incidenti. ✔

Non salvare dati sul dispositivo locale: Non salvare alcun tipo di dato sul PC locale, ma utilizzare i dati presenti sui server o sugli applicativi gestionali. In questo modo il furto di un dispositivo non comporta alcun furto di dati. 

Casa di Cura Privata 'Di Lorenzo' spa
Sede legale • via V. Veneto, 37 - 67051 Avezzano (Aq)
Ingresso utenti • via G. Amendola, 22
tel • 0863.4281 fax • 0863.412446 email • info@dilorenzo.it www.dilorenzo.it
PI/CF • 09037401008

Violazioni della privacy

Valutazione:

Rischio di violazioni della privacy dei pazienti dovute a inadempienze nella gestione dei dati personali.

Impatto:

Perdita di fiducia dei pazienti: Le violazioni della privacy possono erodere la fiducia dei pazienti nella struttura sanitaria, compromettendo la relazione tra il personale medico e i pazienti. Questo può influire negativamente sulla partecipazione e sulla cooperazione dei pazienti nel loro percorso di cura.

Rischi legali e sanzioni: Violare le normative sulla privacy dei dati può portare a azioni legali da parte dei pazienti colpiti o delle autorità di regolamentazione. Ciò potrebbe comportare pesanti sanzioni finanziarie e danni all'immagine della struttura sanitaria.

Danno alla reputazione: La pubblicità negativa derivante da violazioni della privacy può danneggiare la reputazione della casa di cura, rendendo più difficile attirare nuovi pazienti e mantenere rapporti positivi con la comunità.

Misure

Politiche e procedure chiare: Definire politiche e procedure chiare per la gestione e la protezione dei dati personali dei pazienti. Assicurarsi che tutto il personale sia formato e rispetti queste politiche. ✔
Formazione continua: Fornire formazione continua al personale sulla gestione sicura dei dati personali e sulla conformità alle leggi sulla privacy. Mantenere il personale informato sui cambiamenti normativi e sulle migliori pratiche nel settore. ✔
Accesso limitato: Implementare controlli di accesso appropriati per garantire che solo il personale autorizzato abbia accesso ai dati sensibili dei pazienti. ✔
Auditing e monitoraggio: Condurre audit regolari per verificare l'aderenza alle politiche di sicurezza dei dati e monitorare l'accesso ai dati sensibili. Identificare e affrontare prontamente eventuali comportamenti non conformi. ✔
Crittaggio dei dati: Crittografare i dati sensibili dei pazienti, sia durante la trasmissione che durante la conservazione. Questa misura aggiuntiva di sicurezza rende più difficile l'accesso non autorizzato ai dati anche in caso di violazioni.
Notifica tempestiva: Implementare un piano di risposta alle violazioni dei dati che comprenda procedure per la notifica tempestiva alle autorità di regolamentazione e ai pazienti interessati in caso di violazione della privacy.
Revisione delle politiche di conservazione dei dati: Rivedere e aggiornare regolarmente le politiche di conservazione dei dati per garantire che i dati siano conservati solo per il tempo necessario e vengano eliminati in modo sicuro quando non sono più necessari.

Attacchi informatici

Valutazione:

Rischio di attacchi informatici, come malware o ransomware, che potrebbero compromettere l'integrità e la disponibilità dei dati sanitari.

Impatto:

Compromissione dell'integrità dei dati: Gli attacchi informatici, come malware o ransomware, possono compromettere l'integrità dei dati sanitari, alterandoli in modo non autorizzato. Questo può portare a decisioni errate basate su informazioni manipolate.

Perdita di disponibilità dei dati: Un attacco informatico può causare la perdita di accesso ai dati sanitari, influenzando negativamente la continuità operativa della struttura sanitaria. L'indisponibilità dei dati può avere conseguenze critiche durante situazioni di emergenza o necessità di intervento rapido.

Violazione della privacy: Un attacco informatico può portare alla divulgazione non autorizzata di dati sanitari sensibili, violando la privacy dei pazienti e potenzialmente esponendoli a rischi quali il furto di identità.

Misure

Utilizzo di software antivirus e antimalware: Installare e mantenere aggiornato un software antivirus e antimalware per rilevare e prevenire l'infezione da malware. Questi strumenti possono individuare e neutralizzare minacce informatiche prima che possano compromettere i dati. ✔

Aggiornamenti regolari dei sistemi: Mantenere tutti i sistemi, inclusi sistemi operativi e software di sicurezza, aggiornati con le ultime patch di sicurezza. Gli aggiornamenti regolari possono correggere vulnerabilità e migliorare la resistenza del sistema agli attacchi. ✔

Backup regolari e archiviazione offline: Effettuare backup regolari dei dati sanitari e conservarli in un luogo offline. In caso di attacco ransomware, avere copie dei dati offline può permettere il ripristino senza dover pagare un riscatto. ✔

Sicurezza della rete: Implementare misure di sicurezza avanzate, come firewall e sistemi di rilevamento delle intrusioni, per proteggere la rete da accessi non autorizzati e attacchi informatici. ✔

Formazione del personale: Fornire formazione regolare al personale sulla sicurezza informatica, compresi avvertimenti sui rischi di phishing e pratiche sicure per l'utilizzo di dispositivi elettronici. La consapevolezza del personale è fondamentale per prevenire azioni che potrebbero portare a compromissioni della sicurezza. ✔

Politiche di accesso e controllo degli utenti: Implementare politiche di accesso basate sui ruoli e limitare l'accesso ai dati solo al personale autorizzato. Monitorare e controllare gli account utente per prevenire accessi non autorizzati. ✔

Pianificazione delle risposte agli incidenti: Avere un piano dettagliato di risposta agli incidenti che stabilisca le azioni da intraprendere in caso di attacco informatico. Questo piano dovrebbe includere la comunicazione con le autorità competenti e il ripristino rapido dei dati e dei sistemi. 🏗

Errori umani

Valutazione:

Rischio di errori umani nella gestione dei dati, ad esempio invio di informazioni a persone sbagliate o registrazione di dati inaccurati.

Impatto:

Violazione della privacy: Gli errori umani possono portare alla divulgazione non autorizzata di informazioni sensibili, violando la privacy dei pazienti e causando preoccupazioni etiche.

Dati inesatti: Errori nella registrazione dei dati possono compromettere l'accuratezza e l'affidabilità delle informazioni sanitarie. Questo può influire negativamente sulla qualità delle cure fornite e sulla presa di decisioni cliniche.

Perdita di fiducia: La presenza di errori ripetuti nella gestione dei dati può erodere la fiducia dei pazienti nella struttura sanitaria. La perdita di fiducia può influenzare la reputazione della struttura e ridurre la partecipazione dei pazienti.

Misure

Formazione del personale: Fornire formazione approfondita al personale sulla corretta gestione dei dati sanitari, enfatizzando l'importanza della precisione e della riservatezza. La formazione continua può contribuire a ridurre gli errori umani. ✔

Procedure standardizzate: Implementare procedure standardizzate per la gestione dei dati, comprese linee guida chiare sulla registrazione e la condivisione delle informazioni. Queste procedure dovrebbero essere facilmente accessibili e comprensibili per tutto il personale. 🏗

Verifiche incrociate e revisioni: Implementare controlli incrociati regolari e revisioni dei dati da parte di personale qualificato. Questo può contribuire a individuare e correggere errori prima che causino problemi più gravi. ✔

Sistemi di notifica di errori: Implementare un sistema di notifica degli errori che consenta al personale di segnalare tempestivamente eventuali inesattezze o divulgazioni non autorizzate. Questo favorisce la trasparenza e la correzione immediata degli errori. ✔

Accesso basato sui ruoli: Limitare l'accesso ai dati solo al personale autorizzato e basato sui ruoli. Ciò riduce la possibilità di errori da parte di personale non autorizzato e assicura che solo coloro che necessitano di determinate informazioni abbiano accesso ad esse. ✔

Tecnologia di validazione automatica: Utilizzare sistemi informatici con funzionalità di validazione automatica per rilevare e segnalare errori comuni durante la registrazione dei dati. Questi controlli automatici possono agire come ulteriore strato di protezione. 🗓

Auditing e monitoraggio: Implementare procedure regolari di auditing e monitoraggio per valutare la qualità dei dati e individuare eventuali discrepanze. L'identificazione tempestiva degli errori consente una rapida correzione. ✔

Mancanza di formazione del personale

Valutazione:

Rischio derivante dalla mancanza di formazione del personale sulla sicurezza dei dati e sulla gestione delle informazioni sanitarie sensibili.

Impatto:

Violazioni della privacy: La mancanza di formazione può portare a comportamenti inconsapevoli da parte del personale, causando violazioni della privacy dei pazienti attraverso la divulgazione non autorizzata di informazioni sensibili.

Rischio di phishing e attacchi informatici: Un personale non addestrato potrebbe essere più suscettibile agli attacchi di phishing e a pratiche di sicurezza informatica scadenti, aumentando il rischio di accessi non autorizzati e compromissione dei dati.

Gestione inadeguata dei dati: La mancanza di competenze nella gestione delle informazioni sanitarie può portare a errori umani, registrazione inesatta dei dati e una scarsa comprensione delle implicazioni legali e etiche della gestione delle informazioni sanitarie.

Misure

Programmi di formazione regolari: Implementare programmi di formazione regolari sulle norme di sicurezza dei dati e sulla gestione delle informazioni sanitarie. Questi programmi dovrebbero essere obbligatori per tutto il personale e dovrebbero essere aggiornati regolarmente per includere nuove minacce e procedure. ✔
Sensibilizzazione sulla sicurezza informatica: Fornire formazione specifica sulla sicurezza informatica, inclusa l'identificazione di minacce come phishing, malware e altre tattiche di attacco. Migliorare la consapevolezza del personale è fondamentale per prevenire attacchi informatici. ✔
Simulazioni di phishing: Condurre simulazioni di phishing per valutare la resistenza del personale agli attacchi di phishing. Questo tipo di esercitazione può aiutare a identificare aree di debolezza e migliorare la preparazione del personale.
Materiali educativi chiari: Fornire materiali educativi chiari e facilmente accessibili che spieghino le politiche di sicurezza dei dati, le normative sulla privacy e le migliori pratiche nella gestione delle informazioni sanitarie.
Incentivi per la conformità: Implementare incentivi per il personale che dimostra elevati standard di sicurezza dei dati e conformità alle politiche di gestione delle informazioni sanitarie. Questi incentivi possono includere riconoscimenti, premi o opportunità di sviluppo professionale.
Valutazioni delle competenze: Condurre valutazioni regolari delle competenze del personale per garantire che abbiano la conoscenza e le abilità necessarie per gestire in modo sicuro le informazioni sanitarie.
Coinvolgimento del personale: Coinvolgere attivamente il personale nella definizione delle politiche di sicurezza dei dati. Questo può aumentare la consapevolezza e l'adesione alle pratiche di sicurezza, poiché il personale si sentirà coinvolto nel processo decisionale.

Insider Threats

Valutazione:

Rischio derivante dalle minacce interne, come il cattivo uso intenzionale delle informazioni da parte di personale autorizzato.

Impatto:

Violazione della privacy dei pazienti: Un insider potrebbe abusare intenzionalmente delle informazioni sanitarie dei pazienti, violando la loro privacy e causando danni reputazionali alla struttura sanitaria.

Divulgazione non autorizzata di dati sensibili: Il cattivo uso intenzionale delle informazioni potrebbe portare alla divulgazione non autorizzata di dati sensibili, aumentando il rischio di furto di identità e di altre violazioni della sicurezza.

Danni alla reputazione: Le azioni malevole di un insider possono danneggiare la reputazione della struttura sanitaria, minando la fiducia dei pazienti e degli altri stakeholder.

Perdite finanziarie: Le minacce interne possono causare perdite finanziarie attraverso azioni come la vendita di informazioni sensibili o la manipolazione di dati a fini personali o competitivi.

Misure

Implementazione di controlli di accesso granulari: Limitare l'accesso alle informazioni sanitarie solo alle persone che ne hanno effettivamente bisogno per svolgere le proprie mansioni. Questo può ridurre il rischio di cattivo uso intenzionale delle informazioni. ✔

Monitoraggio delle attività degli utenti: Implementare sistemi di monitoraggio delle attività degli utenti per rilevare comportamenti anomali o accessi non autorizzati. L'analisi delle anomalie può aiutare a individuare potenziali minacce interne. ✔

Formazione sulla sicurezza: Fornire formazione continua sulle politiche di sicurezza e sulle conseguenze del cattivo uso delle informazioni. Sensibilizzare il personale sulle minacce interne può contribuire a prevenire tali comportamenti. ✔

Segnalazione anonima: Implementare un sistema di segnalazione anonima che consenta al personale di segnalare comportamenti sospetti senza paura di ritorsioni. Questo può facilitare la rilevazione tempestiva di minacce interne. 📅

Revisioni periodiche dei privilegi di accesso: Periodicamente rivedere e aggiornare i privilegi di accesso in base alle responsabilità correnti dei dipendenti. Ciò riduce il rischio di abusi legati a privilegi di accesso non necessari. ✔

Auditing regolare: Condurre audit regolari dei dati e delle attività degli utenti per identificare eventuali violazioni o anomalie. L'auditing può essere un elemento chiave nella prevenzione e nella risposta alle minacce interne. ✔

Pianificazione delle risposte agli incidenti: Avere un piano dettagliato di risposta agli incidenti che includa procedure specifiche per gestire minacce interne. Questo può aiutare a mitigare tempestivamente gli impatti di un'azione malevola interna. ✔

Casa di Cura Privata 'Di Lorenzo' spa
Sede legale • via V. Veneto, 37 - 67051 Avezzano (Aq)
Ingresso utenti • via G. Amendola, 22
tel • 0863.4281 fax • 0863.412446 email • info@dilorenzo.it www.dilorenzo.it
PI/CF • 09037401008

Perdita dei dati

Valutazione:

Rischio di perdita di dati a causa della mancanza di procedure di backup efficaci e di un piano di ripristino in caso di incidente.

Impatto:

Perdita irreversibile dei dati: La mancanza di procedure di backup può portare alla perdita permanente di dati critici in caso di incidenti come malfunzionamenti hardware, errori umani o attacchi informatici.

Interruzione operativa prolungata: In assenza di un piano di ripristino, la struttura sanitaria potrebbe sperimentare un'indisponibilità prolungata dei dati in seguito a un incidente, con possibili impatti sulla continuità operativa e sulla qualità delle cure fornite.

Riduzione della fiducia dei pazienti: La perdita di dati può minare la fiducia dei pazienti nella capacità della struttura sanitaria di gestire e proteggere le loro informazioni, influenzando negativamente la reputazione della struttura.

Misure

Implementazione di procedure di backup robuste: Stabilire procedure di backup regolari e affidabili per assicurare la copia sicura e completa dei dati critici. I backup dovrebbero essere eseguiti su base regolare e includere tutti i dati necessari per la continuità operativa. ✔

Archiviazione offline dei backup: Conservare le copie di backup offline, lontano dai sistemi principali, per proteggerle da minacce come ransomware o attacchi informatici che potrebbero colpire i dati online. ✔

Pianificazione di backup automatizzata: Automatizzare il processo di backup per ridurre al minimo il rischio di errori umani e garantire che i backup siano eseguiti regolarmente senza dipendere dalla manuale esecuzione da parte del personale. ✔

Verifica periodica dei backup: Effettuare verifiche periodiche dei backup per assicurarsi che siano completi, integri e recuperabili. Queste verifiche dovrebbero essere parte integrante della gestione della sicurezza informatica. ✔

Elaborazione di un piano di ripristino: Creare un piano di ripristino dettagliato che delinei le procedure da seguire in caso di perdita di dati. Questo piano dovrebbe essere testato regolarmente per garantire che sia efficace e che il personale sia pronto a eseguirlo in situazioni di emergenza. ✔

Coinvolgimento del personale: Coinvolgere il personale nella comprensione e nell'attuazione delle procedure di backup e ripristino. Il personale dovrebbe essere a conoscenza dell'importanza di tali processi per garantire la sicurezza dei dati. 📅

Monitoraggio continuo: Implementare sistemi di monitoraggio continuo per rilevare eventuali anomalie nei dati o nei processi di backup. Un monitoraggio proattivo può contribuire a identificare e risolvere i problemi prima che causino danni significativi. ✔

Casa di Cura Privata 'Di Lorenzo' spa
Sede legale • via V. Veneto, 37 - 67051 Avezzano (Aq)
Ingresso utenti • via G. Amendola, 22
tel • 0863.4281 fax • 0863.412446 email • info@dilorenzo.it www.dilorenzo.it
PI/CF • 09037401008

Obsolescenza tecnologica

Valutazione:

Rischio derivante dalla presenza di tecnologie obsolete o non aggiornate, che potrebbero presentare vulnerabilità di sicurezza

Impatto:

Aumento del rischio di vulnerabilità: Le tecnologie obsolete spesso non beneficiano degli ultimi aggiornamenti di sicurezza, aumentando il rischio di vulnerabilità. Queste vulnerabilità possono essere sfruttate da attaccanti per compromettere la sicurezza dei dati.

Interruzioni dei servizi: Le tecnologie obsolete potrebbero diventare instabili o non funzionare correttamente, causando interruzioni dei servizi. Ciò potrebbe influire sulla qualità delle cure fornite e sulla continuità operativa della struttura sanitaria.

Non conformità alle normative: L'uso di tecnologie obsolete potrebbe render difficile o impossibile rispettare le normative sulla privacy e la sicurezza dei dati, portando a potenziali violazioni normative e sanzioni.

Misure

Inventario e valutazione delle tecnologie: Condurre un inventario completo delle tecnologie utilizzate e valutarne la sicurezza. Identificare le tecnologie obsolete o non supportate e pianificare l'aggiornamento o la sostituzione. ✔

Pianificazione degli aggiornamenti: Stabilire una pianificazione regolare per gli aggiornamenti di software e hardware. Assicurarsi che tutte le tecnologie siano mantenute con le ultime patch di sicurezza per ridurre il rischio di vulnerabilità. 

Aggiornamenti del sistema operativo: Mantenere i sistemi operativi aggiornati con le versioni più recenti, poiché spesso contengono correzioni di sicurezza essenziali. Nel caso di sistemi operativi obsoleti, pianificare la migrazione a versioni più recenti. 

Aggiornamento delle applicazioni: Assicurarsi che tutte le applicazioni, comprese quelle specifiche per la gestione delle informazioni sanitarie, siano regolarmente aggiornate per correggere eventuali vulnerabilità e migliorare la sicurezza. 

Sostituzione delle tecnologie obsolete: Dove possibile, pianificare la sostituzione delle tecnologie obsolete con soluzioni più moderne e sicure. Questo può includere l'acquisto di nuove attrezzature o la migrazione verso piattaforme più recenti. ✔

Monitoraggio del ciclo di vita delle tecnologie: Implementare un sistema di monitoraggio del ciclo di vita delle tecnologie, che includa l'identificazione delle scadenze di supporto del produttore. Ciò aiuta a prevedere e gestire proattivamente la sostituzione di dispositivi obsoleti. 

Consulenza di esperti: Coinvolgere consulenti di sicurezza informatica o esperti del settore per valutare la sicurezza delle tecnologie utilizzate e fornire consulenze sulla gestione del rischio legato alle tecnologie obsolete. ✔

Pianificazione per il futuro: Integrare una strategia di pianificazione a lungo termine per garantire che la struttura sanitaria sia in grado di rimanere aggiornata con le tecnologie emergenti e rimuovere gradualmente quelle obsolete.

Compliance Normativa

Valutazione:

Rischio di non conformità con le normative e le leggi sulla privacy, con conseguente esposizione a sanzioni legali.

Impatto:

Sanzioni legali e multe: La mancanza di conformità con le normative sulla privacy può portare a sanzioni legali e multe significative, imposte dalle autorità di regolamentazione. Queste sanzioni possono avere impatti finanziari notevoli sulla struttura sanitaria.

Perdita di fiducia: La non conformità può danneggiare la fiducia dei pazienti e delle loro famiglie nella capacità della struttura sanitaria di proteggere le loro informazioni personali. Ciò può influire negativamente sulla reputazione e sulla partecipazione dei pazienti.

Perdita di opportunità di business: L'essere non conformi alle normative sulla privacy potrebbe comportare la perdita di opportunità di business, ad esempio, partnership con altre organizzazioni sanitarie o collaborazioni con fornitori di servizi.

Misure

Conoscenza e aderenza alle leggi vigenti: Mantenere una conoscenza approfondita delle leggi sulla privacy pertinenti al settore sanitario e assicurarsi che la struttura sanitaria sia pienamente informata e aderente a queste leggi.

Nomina di un responsabile della protezione dei dati (DPO): Se richiesto dalle normative, nominare un DPO responsabile della protezione dei dati, con il compito di monitorare e garantire la conformità alle normative sulla privacy.

Valutazione periodica della conformità: Condurre regolarmente valutazioni della conformità rispetto alle normative sulla privacy per identificare eventuali aree di non conformità e intraprendere azioni correttive tempestive.

Politiche e procedure chiare: Sviluppare e implementare politiche e procedure chiare sulla gestione delle informazioni sanitarie e sulla privacy dei pazienti. Assicurarsi che tutto il personale sia a conoscenza e segua queste politiche.

Formazione continua del personale: Fornire formazione regolare a tutto il personale sulla protezione della privacy e sulle leggi vigenti. La consapevolezza del personale è fondamentale per ridurre il rischio di violazioni della privacy.

Consulenza legale: Coinvolgere consulenti legali specializzati in privacy e sicurezza delle informazioni per garantire che la struttura sanitaria sia pienamente conforme alle leggi vigenti.

Implementazione di misure di sicurezza: Mettere in atto misure di sicurezza tecniche e organizzative per proteggere le informazioni sanitarie e garantire la riservatezza dei dati, come l'uso di crittografia, controlli di accesso e monitoraggio delle attività degli utenti.

Gestione degli incidenti di sicurezza: Avere un piano dettagliato per la gestione degli incidenti di sicurezza, che includa la notifica tempestiva delle violazioni delle informazioni sanitarie alle autorità e ai pazienti interessati, come richiesto dalle leggi vigenti

Disastro ambientale

Valutazione:

Rischio derivante da calamità naturali come allagamenti, incendi o terremoti.

Impatto:

Perdita irreparabile dei dati: Le calamità naturali, come allagamenti o incendi, possono causare la distruzione fisica degli ambienti e delle infrastrutture, portando alla perdita irreparabile di dati sanitari critici.

Interruzione dei servizi: Calamità come terremoti o incendi possono causare danni alle infrastrutture fisiche, interrompendo i servizi sanitari e compromettendo la capacità della struttura di fornire cure ai pazienti.

Rischio per la sicurezza fisica: Alcune calamità naturali possono mettere a rischio la sicurezza fisica dei pazienti e del personale, con possibili impatti sulla salute e sulla sicurezza.

Perdita di attrezzature mediche: Incidenti come allagamenti possono danneggiare o distruggere attrezzature mediche costose, con conseguenti costi di riparazione o sostituzione.

Misure

Pianificazione della continuità operativa: Sviluppare e implementare un piano di continuità operativa che includa procedure per la gestione delle calamità naturali. Ciò dovrebbe coprire il ripristino delle operazioni, la protezione dei dati e la sicurezza del personale e dei pazienti.

Siti di backup fuori sede: Mantenere siti di backup fuori sede per i dati critici, garantendo che le informazioni sanitarie siano replicate in un luogo sicuro e accessibile in caso di calamità.

Strutture resistenti alle calamità: Valutare e rafforzare le strutture fisiche della struttura sanitaria per renderle più resistenti alle calamità naturali. Ciò può includere la protezione contro incendi, alluvioni e altri rischi specifici della zona.

Piani di evacuazione: Sviluppare piani di evacuazione e procedure di sicurezza per garantire la protezione del personale e dei pazienti in caso di calamità naturale imminente. Esercitazioni regolari possono contribuire a preparare il personale a rispondere efficacemente.

Sistemi di allarme precoce: Implementare sistemi di allarme precoce per ricevere notifiche tempestive in caso di calamità naturale, consentendo una risposta rapida e l'evacuazione, se necessario.

Collaborazione con le autorità locali: Collaborare con le autorità locali e i servizi di emergenza per garantire una risposta coordinata in caso di calamità. Mantenere una comunicazione regolare può facilitare la pianificazione e la risposta durante situazioni di emergenza.

Aggiornamento periodico dei piani di emergenza: Periodicamente, rivedere e aggiornare i piani di emergenza in base alle nuove informazioni, alle esperienze passate e ai cambiamenti nell'infrastruttura e nelle risorse disponibili

Monitoraggio e Revisione

La Revisione del presente DPS verrà effettuata quando, per mutate circostanze, se ne dovesse ravvisare l'esigenza ed annualmente sarà verificato lo stato di attuazione delle misure in corso di implementazione e di quelle pianificate e da pianificare.

Procedure per la documentazione e la notifica di eventuali violazioni della sicurezza

La registrazione degli eventi anomali viene effettuata attraverso il Sistema di Gestione Qualità con l'apertura di una Non Conformità, annotando anche le caratteristiche dell'evento anomalo, la sua origine, gli effetti provocati e la risoluzione del problema. Nel caso di violazioni di particolare gravità si apre una segnalazione ai sensi del D.L.vo 231/2001 e si attiva la segnalazione del Data Breach.