

Informazioni sul PIA

Data di creazione

20/05/2018

Contesto

Panoramica

Quale è il trattamento in considerazione?

Trattamento dei dati operato presso la struttura della Casa di Cura Figlie Santa Maria di Leuca, Via Tiberina, 173 - 001 88 Roma

Quali sono le responsabilità legate al trattamento?

Le responsabilità sono quelle legate alla cura e sicurezza dei dati sensibili dei pazienti della struttura, oltre che ai dati personali dei dipendenti, dei fornitori e dei clienti, censiti per le normali operazioni commerciali e amministrative della struttura.

Ci sono standard applicabili al trattamento?

Gli **standard** applicati sono corrispondenti alle modalità operative poste in essere, in base alle quali tutti i dati vengono acquisiti dalla amministrazione, che è composta da n. 5 Religiose che operano su base informatica utilizzando terminali con sistemi di sicurezza.

I dati raccolti vengono gestiti unicamente per l'organizzazione del lavoro e la formazione della cartella clinica, ove necessaria o, per le visite ambulatoriali, svolte all'interno della struttura.

Per quanto concerne le cartelle cliniche, si rappresenta che le stesse vengono compilate con l'intervento di figure professionali, che devono conoscere i dati sensibili per l'esecuzione dei loro interventi, per lo svolgimento delle loro prestazioni e per la somministrazione delle cure.

Le appartenenti alla struttura amministrativa vivono nella Casa sita all'interno della Clinica e sono particolarmente garantite dalla vocazione che ha condotto alla scelta religiosa e dalla professionalità rappresentata da molti anni di servizio irreprensibile in tali funzioni.

Anche riguardo al personale infermieristico, valgono le medesime considerazioni svolte rispetto per quello amministrativo. In riferimento ai professionisti che svolgono la loro attività all'interno della struttura, si rileva che sono rappresentati da professori e medici che in funzione dell'attività svolta sono tenuti al segreto professionale e, inoltre, tutte le documentazioni e le cartelle restano presso la struttura e niente viene portato all'esterno.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati sono quelli identificativi della persona, ai fini amministrativi e fiscali, nonché gli altri riguardanti lo stato di salute e le problematiche pregresse.

Non viene effettuato nessun trattamento di dati relativi ad orientamenti politici, sessuali e religiosi.

Com'è il ciclo di vita del trattamento dei dati?

I dati anagrafici vengono raccolti per tutti non appena il soggetto entra in contatto con la struttura, sia ai fini amministrativi, che a quelli fiscali.

Poi, se trattasi di fornitori o personale dipendente, non vengono svolte ulteriori valutazioni e approfondimenti, mentre nel caso di pazienti è necessario approfondire le patologie e le motivazioni del ricorso ai servizi offerti dalla struttura. Questo esame, che potrà concretizzarsi in una cartella clinica o, semplicemente, in una visita

specialistica, viene svolta dal personale medico specialistico che, nel primo caso, diventa un anello di un processo più complesso, mentre nel secondo è il terminale di una attività che termina con una visita specialistica.

Quali sono le risorse di supporto ai dati?

Le risorse di supporto sono costituite da un data base che contiene tutti gli elementi identificativi necessari per la gestione amministrativa e fiscale degli interessati. l'accesso a tali funzioni è limitato a coloro che funzionalmente hanno necessità di accedervi e è salvaguardato da password.

Per quanto riguarda le cartelle cliniche cartacee, invece, le stesse sono custodite all'interno di un'area riservata, non accessibile e vengono rese disponibili per il tempo necessario al trattamento.

Principi Fondamentali

Proporzionalità, necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento sono dettati esclusivamente dalle normative fiscali e previdenziali vigenti, nonché dalla necessità di procedere ai trattamenti sanitari, nell'ambito dei protocolli medici previsti dalla legislazione vigente.

Quali sono le basi legali che rendono il trattamento legittimo?

Il trattamento è reso legittimo dal consenso espresso che viene rilasciato dalle persone che vengono censite e che si trovano nella necessità di fare ricorso ai servizi medici e chirurgici offerti dalla struttura.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati (minimizzazione dei dati)?

Ogni dato raccolto è direttamente e specificatamente funzionale alle necessità per le quali è stato richiesto. in particolare, ai fini amministrativi e fiscali, vengono richiesti i dati necessari alla compilazione della fattura e dei dati correlati che sono richiesti dalla vigente normativa.

Per quanto riguarda le cure, i medici richiedono quelle che sono le patologie trascorse, lo stato di salute e le problematiche attuali, con tutti gli approfondimenti necessari per le cure che debbono essere effettuate.

I dati sono accurati e mantenuti aggiornati?

I dati sono presi con cura e riservatezza e vengono mantenuti per lo svolgimento degli obblighi imposti dalle vigenti normative.

Gli aggiornamenti vengono effettuati quando il soggetto rinnova il contatto con la struttura o quando norme imposte dalla legislazione lo richiedono.

Non viene svolto un aggiornamento autonomo, se non obbligati dalla normative vigente.

Quale è la durata della conservazione dei dati?

La durata della conservazione è legata alla normativa fiscale vigente e alla necessità di svolgere trattamenti sanitari sul paziente.

Controlli per proteggere i diritti personali dei soggetti interessati

I soggetti interessati come sono informati del trattamento?

I soggetti interessati sono informati del trattamento attraverso la sottoscrizione di un apposito documento nel quale sono evidenziate le ragioni della raccolta dei dati e attraverso il documento sulla privacy.

Come si ottiene il consenso dei soggetti interessati?

Il consenso si ottiene attraverso la sottoscrizione del documento di cui al precedente paragrafo.

I soggetti interessati come esercitano i loro diritti di accesso alla portabilità dei dati?

La portabilità dei dati è esercitata, come evidenziato anche nel documento privacy, attraverso la richiesta da svolgere all'indirizzo di posta elettronica indicato sullo stesso.

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

Il diritto alla rettifica e alla cancellazione come evidenziato anche nel documento privacy, attraverso la richiesta da svolgere all'indirizzo di posta elettronica indicato sullo stesso.

i soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

Per ottenere la restrizione e l'obiezione è sufficiente presentare una richiesta alla mail indicata sul documento privacy, oppure provvedere alla richiesta direttamente presso l'amministrazione della casa di cura.

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

Gli obblighi dei responsabili sono specificatamente previsti in un contratto e sono conformi a quelli previsti dalla vigente normativa

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

Non vengono svolte attività al di fuori della Comunità europea

Rischi

Controlli esistenti o pianificati

Svolgimento controlli

I controlli sono svolti attraverso una specifica valutazione dei processi ed un esame a campione sui dati raccolti

Accesso illegittimo ai dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio si dovesse realizzare?

I rischi sono relativi principalmente alla divulgazione di dati sanitari personali

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Non si riscontrano attualmente minacce incombenti sul trattamento dei dati

Quali sono le fonti di rischio?

Il sistema di raccolta e conservazione dei dati è molto sicuro, l'unico rischio valutabile è quello eventualmente legato al

comportamento doloso di un professionista operante all'interno della struttura.

Quali dei controlli identificati contribuiscono a gestire il rischio?

Presenza di password e conservazione dei documenti.

Come stimeresti la gravità del rischio, specialmente riguardo i potenziali impatti e i controlli pianificati?

Molto basso

Come stimeresti la probabilità del rischio, specialmente riguardo le minacce, fonti di rischio e i controlli

pianificati?

Trascurabile

Modifiche indesiderate dei dati

Quali impatti ci sarebbero sui soggetti interessati se il rischio si dovesse concretizzare?

Pubblicazione di dati sensibili, con diversi impatti in funzione delle situazioni personali degli interessati

Quali sono le principali minacce che possono portare al rischio?

Non si rilevano minacce particolari, anche quelle legate ad eventuali comportamenti fraudolenti degli operatori esterni, sono molto limitate dai dispositivi di sicurezza utilizzati

Quali sono le fonti di rischio?

Solo i rischi di carattere generale, non si rilevano rischi particolari.

Quali dei controlli identificati contribuiscono a gestire il rischio?

Inserimento di password ai terminali, conservazione delle stesse in modo sicuro e conservazione dei fascicoli in area riservata, accessibile solo al personale interno.

Come stimeresti la gravità del rischio, in particolare riguardo l'impatto potenziale e i controlli pianificati?

Irrelevanti

Come stimeresti la probabilità del rischio, specialmente riguardo minacce, fonti di rischio e controlli pianificati?

Irrelevanti

Scomparsa di dati

Quale potrebbe essere l'impatto sui soggetti interessati se il rischio dovesse realizzarsi?

nessuno

Quali sono le minacce che potrebbero portare al rischio?

problemi informatici

Quali sono le fonti di rischio?

problemi informatici e furto dei dati

Quali dei controlli identificati contribuisce a gestire il rischio?

Tutti quelli posti in essere

Come stimeresti la gravità del rischio, specialmente riguardo il potenziale impatto e i controlli pianificati?

Trascurabili

Come stimeresti la probabilità del rischio, specialmente rispetto le minacce, fonti di rischio e i controlli pianificati?

Trascurabile

Piano d'azione

Principi fondamentali

Nessun piano d'azione registrato.

Controlli esistenti o pianificati

I controlli sono esercitati ad ogni accesso al sistema e ad ogni singolo prelievamento di documentazione

Rischi

I controlli esercitati sono atti ad eliminare rischi di carattere generico e specifico sui dati trattati