INTRODUZIONE

Casa di Cura Villa Dei Gerani Dott. A. Ricevuto S.r.l., Titolare del trattamento, si impegna nel garantire elevati livelli di protezione nelle operazioni di trattamento dei dati personali, siano essi riferiti al proprio personale interno, piuttosto che agli utenti (pazienti e loro familiari) e fornitori.
I principi fondamentali della legislazione vigente in tema di privacy/tutela dei dati personali sono stati analizzati in riferimento ai servizi ed attività promossi ed erogati da Casa di Cura Villa Dei Gerani Dott. A. Ricevuto S.r.l.. Da tale analisi deriva la **POLITICA PER LA PROTEZIONE DEI DATI PERSONALI** - che recepisce e contestualizza tali principi. In particolare si fa riferimento al: - **Regolamento Ue 2016/679**, noto come GDPR (General Data Protection Regulation) – al **Codice Privacy** - D.Lgs. 196/03 così come modificato dal D.Lgs. 101/18 – alle Linee guida Dossier Sanitario Elettronico.
La CASA DI CURA VILLA DEI GERANI DOTT. A. RICEVUTO S.R.L. offre alla POLITICA la massima visibilità verso il personale interno (anche tramite formazione) e verso le terze parti (utenti/fornitori/collaboratori). In coerenza sia con la Missione e Valori aziendali, sia con il contesto in cui opera Casa di Cura -espresso nel Sistema Qualità certificato ISO9001 -, e sulla base della presente Politica, la Direzione riconosce come scelta strategica lo sviluppo di un sistema di gestione per la protezione dei dati personali.
Operando nel settore sanitario sono principalmente i dati personali e sensibili dei Pazienti ad essere oggetto di attenzione ed opportuno trattamento.

DEFINIZIONI

Ai sensi della presente Politica si riportano i principali termini in uso ed il loro significato: • **interessato** è qualsiasi persona fisica a cui appartengono i dati oggetto di trattamento
• **consenso al trattamento dei dati** è una dichiarazione di approvazione volontaria e legalmente vincolante
• **dati personali** sono tutte le informazioni che riguardano una persona fisica identificata o identificabile. Una persona è identificabile se, ad esempio, può essere individuata attraverso la combinazione con conoscenze ulteriori anche solo casualmente rinvenibili
• **trattamento dei dati personali** è l'attività effettuata sui dati (per es. la raccolta, la registrazione, l'alterazione, il trasferimento, il blocco, la cancellazione e la consultazione)

SCOPO E OBIETTIVI

La direzione di Casa di Cura Villa Dei Gerani Dott. A. Ricevuto S.r.l. ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Privacy.
Lo scopo della presente policy è di garantire la tutela e la protezione dei dati personali gestiti nell'ambito delle attività della Casa di Cura e la minimizzazione dei rischi connessi alla protezione dei dati, interni o esterni, intenzionali o accidentali, in accordo con le indicazioni fornite dal D.Lgs. 196/03 e del Reg. UE 679/2016.

CAMPO DI APPLICAZIONE

La presente politica si applica indistintamente a tutti gli organi e i livelli della Casa di Cura. L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Privacy.
In CASA DI CURA VILLA DEI GERANI DOTT. A. RICEVUTO S.R.L. sussistono due macro ambiti in tema di trattamento di dati: 1. trattamento dei dati di dipendenti, fornitori, consulenti esterni;

collaboratori 2. trattamento dei dati dell'Utente. Si pensi, in particolare, ai dati dei pazienti, con i quali il personale della Casa di Cura viene a contatto nell'erogazione delle proprie attività.

PRINCIPI SULLA PROTEZIONE DEI DATI

I dati personali devono essere trattati in modo lecito e tale da salvaguardare i diritti alla riservatezza dell'interessato.
A tal fine devono essere osservati i seguenti principi sulla protezione dei dati.

- Finalità del trattamento dei dati / limitazioni all'uso dei dati

In linea di principio, i dati personali possono essere trattati solo per gli scopi definiti prima della raccolta dei medesimi. Modifiche successive allo scopo che non hanno una stretta connessione oggettiva con lo scopo originale sono possibili solo in misura limitata.

- Proporzionalità

Nel trattamento dei dati personali deve essere osservato il principio di proporzionalità. Il trattamento dei dati è proporzionale solo se è idoneo, necessario e ragionevole per il conseguimento di uno scopo legittimo e se i preminenti interessi legittimi dell'interessato non lo impediscano.

- Trasparenza

In linea di principio, gli interessati devono essere informati, obbligatoriamente ed in modo adeguato dal titolare del trattamento, in merito al trattamento dei propri dati personali.

- Minimizzazione dei dati.

Il principio di minimizzazione dei dati parte dall'idea che, salvo poche eccezioni, un titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento.

- Qualità dei dati

I dati personali devono essere raccolti e trattati in modo tale che siano oggettivamente corretti. È necessario adottare misure adeguate per garantire che i dati erronei o incompleti siano corretti, integrati o cancellati.

- Integrità

Ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.

- Disponibilità

L'interessato deve sempre poter effettivamente accedere alle proprie informazioni nel momento in cui lo richieda.

- Confidenzialità del trattamento

I dati personali devono essere protetti dall'accesso a persone non autorizzate. È vietato il trattamento non autorizzato di tali dati. Qualsiasi trattamento effettuato da persone non abilitate a farlo nell'ambito dei propri compiti o non adeguatamente autorizzate non è consentito. In particolare, i dati personali non devono essere trasferiti o resi altrimenti disponibili a persone non autorizzate.

MISURE DI PROTEZIONE DEI DATI

La tutela dei diritti alla riservatezza, con particolare riferimento alle misure tecniche e organizzative per la protezione dei dati personali delle persone interessate, richiede un alto livello di sicurezza delle informazioni.
Per la protezione dei dati personali degli interessati, la Casa di Cura Villa Dei Gerani Dott. A. Ricevuto S.r.l.:

- ha nominato un Responsabile della Protezione dei dati/Data Protection Officer DPO
- si avvale di una serie di tecnologie ed ha implementato un sistema di gestione dotato di procedure aziendali di protezione. (Ad esempio, utilizziamo controlli per l'accesso, firewall,

server protetti ed effettuiamo la crittografia di alcuni tipi di dati come le informazioni relative al Vs stato di salute contenute in cartella clinica).
- viene istituito e tenuto un apposito Registro delle attività di trattamento dei dati che vengono trattati sotto la sua responsabilità.

– Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi viene sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni sono differenziate in base al ruolo ed agli incarichi ricoperti dai singoli individui, in modo che ogni utente possa accedere alle sole informazioni di cui necessita, e sono periodicamente sottoposte a revisione.

–E' incoraggiata la piena consapevolezza delle problematiche relative alla sicurezza delle informazioni in tutto il personale (dipendenti e collaboratori) a partire dal momento della selezione e per tutta la durata del rapporto di lavoro.

– Si previene l'accesso non autorizzato alle sedi e ai singoli locali aziendali dove sono gestite le informazioni e viene garantita la sicurezza delle apparecchiature.

– Viene assicurata la conformità con i requisiti legali e con i principi legati alla sicurezza delle informazioni nei contratti con i fornitori.

– E' stato predisposto un piano di continuità che permetta alla Casa di Cura di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino le conseguenze negative sulla missione aziendale.

– Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.

– Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, riducendo al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.

La direzione identifica, inoltre, tutte le esigenze di sicurezza tramite la **valutazione di impatto sulla protezione dei dati** che consente di acquisire consapevolezza sul livello di esposizione a minacce dei propri sistemi di gestione dei dati.

La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.

I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette ed adeguate misure di sicurezza ed i meccanismi per garantire la protezione dei dati personali.

OBBLIGO DI SEGNALAZIONE DELLE VIOLAZIONI RELATIVE ALLA PROTEZIONE DEI DATI

Nel caso in cui i dati personali vengano trattati in violazione dei principi definiti nella presente Politica, o se soggetti terzi vengano illegalmente a conoscenza dei dati personali oppure vi sia una grave compromissione del trattamento dei dati personali, è necessario attivare la specifica procedura di Data Breach.

DIRITTI DEGLI INTERESSATI

In caso di trattamento di dati personali, secondo il principio di trasparenza, gli interessati devono avere l'opportunità di venirne a conoscenza tempestivamente, a tal fine all'interno del sistema di gestione privacy, sono state predisposte diverse informative ex artt. 13 – 14 GDPR. Gli interessati hanno il diritto di ottenere informazioni e che i dati erronei o incompleti vengano corretti. In ogni momento l'interessato potrà esercitare i propri diritti nei confronti del Titolare del

trattamento, specificamente previsti dal Capo III del Reg. UE 2016/679 (diritto di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, diritto alla portabilità dei dati, diritto di proporre reclamo al Garante per la protezione dei dati).

RUOLI E RESPONSABILITÀ

La responsabilità per l'implementazione e l'osservanza delle norme statutarie e aziendali per la protezione dei dati personali è in capo alla Direzione di Casa di Cura Villa Dei Gerani Dott. A. Ricevuto S.r.l. Tali doveri comprendono, in particolare, l'obbligo di dimostrare la conformità alle norme (l'obbligo di responsabilità accountability).
L'osservanza e l'attuazione della policy coinvolgono:

1-tutto il personale che, a qualsiasi titolo, collabora con l'azienda per svolgere le proprie mansioni tratta dati personali e informazioni che rientrano nel campo di applicazione del Sistema di Gestione Privacy. Tutto il personale è altresì responsabile della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza.
2-tutti i soggetti esterni che intrattengono rapporti e che, collaborando con l'azienda, devono garantire il rispetto dei requisiti contenuti nella presente policy.
3- il Responsabile della Protezione dei dati/Data Protection Officer DPO che ha il compito di vigilare sull'osservanza del GDPR da parte della Casa di Cura.

Chiunque, dipendenti, consulenti e/o collaboratori esterni dell'Azienda, in modo intenzionale o riconducibile a negligenza, disattenda le regole di sicurezza stabilite e in tal modo provochi un danno al Titolare del Trattamento, potrà essere perseguito nelle opportune sedi e nel pieno rispetto dei vincoli di legge e contrattuali.

TERMINI DI CONSERVAZIONE

Il periodo massimo di conservazione dei dati personali risulta intrinsecamente connesso alle finalità per le quali i dati personali sono stati raccolti ed archiviati. All'interno sono specificati i tempi a seconda che variano sulla base dell'ambito del trattamento e della categoria di trattamento. In particolare tutta la documentazione sanitaria contenuta all'interno della cartella clinica viene custodita sine die (cioè anche dopo il decesso del paziente), come da disposto normativo.

RIESAME

La Direzione verificherà periodicamente e regolarmente almeno una volta all'anno o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione Privacy, in modo da assicurare un supporto adeguato all'introduzione di tutte le migliorie necessarie e in modo da favorire l'attivazione di un processo continuo, con cui viene mantenuto il controllo e l'adeguamento della policy in risposta ai cambiamenti dell'ambiente aziendale, dei servizi sanitari, delle condizioni legali.

IMPEGNO DELLA DIREZIONE

La direzione sostiene attivamente le attività inerenti la gestione della privacy tramite un chiaro indirizzo, un impegno evidente, degli incarichi espliciti e il riconoscimento delle responsabilità relative alla sicurezza dei dati.
L'impegno della direzione si attua tramite un sistema di gestione che sia in grado di:

– garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni e che

questi incontrino i requisiti aziendali;
– stabilire i ruoli aziendali e le responsabilità per lo sviluppo e il mantenimento del “Sistema Privacy”;
– fornire risorse sufficienti alla pianificazione, implementazione, organizzazione, controllo, revisione, gestione e miglioramento continuo del Sistema;
– controllare che il Sistema di Gestione sia integrato in tutti i processi aziendali e che procedure e controlli siano sviluppati efficacemente;
– approvare e sostenere tutte le iniziative volte al miglioramento della sicurezza delle informazioni; – attivare programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

“**Riconosciamo la nostra responsabilità e ci impegniamo a proteggere i dati personali che gli utenti ci affidano da perdita, uso improprio o accesso non autorizzato**.”