PROGETTO αδεία
...SICURAMENTE CON VOI...

GEMMA MEDICA S.A.S.

Di BEATRICE PELO

SEDE IN

ACQUAPENDENTE (VT) v. Ilaria Alpi 3

Tel. 075.5997768

mail - info@gemmamedica.com

pec - daddo@pec.it

TRATTAMENTO DATI PERSONALI
DOCUMENTO RIASSUNTIVO DEGLI ADEMPIMENTI NECESSARI PER ADEMPIERE IN MODO CORRETTO AL REGOLAMENTO EUROPEO 2016/679

INDICE

1. CRITERI DI PROTEZIONE DATI PERSONALI - POLITICA

La GEMMA MEDICA sas è una società che offre a medici professionisti uno spazio adeguato per visitare i pazienti e gestire gli appuntamenti con i medesimi. I medici operano come professionisti e non sono legati da alcun vincolo di subalternità con la GEMMA MEDICA sas. I pazienti si relazionano direttamente con i propri professionisti di fiducia. Ogni professionista che opera all'interno degli spazi GEMMA MEDICA è legato al segreto professionale e al codice di condotta vincolante indicato dal proprio Ordine Professionale.

La GEMMA MEDICA sas è comunque impegnata in modo attivo nel rispetto delle normative di legge in merito al trattamento dei dati personali e alla loro circolazione. Allo stesso modo è impegnata nei confronti dei professionisti che operano all'interno dei suoi spazi e dei relativi clienti, per garantire comportamenti corretti in relazione al trattamento dei dati personali, assicurando al tempo stesso l'assistenza necessaria, finalizzata al mantenimento della salute. Ne deriva l'impegno della GEMMA MEDICA sas e dei suoi collaboratori, con particolare riferimento al personale di segreteria, ad assicurare un uso consapevole e serio degli strumenti a disposizione, con particolare riferimento agli strumenti informatici.

La GEMMA MEDICA sas è titolare del trattamento dei dati raccolti durante la propria attività e si impegna a gestire tali dati in modo rispettoso della dignità e della tutela degli interessati, al fine di garantire la migliore tutela della loro salute.

Se necessario il Titolare si impegna a nominare un numero adeguato di Contitolari e di Responsabili del trattamento e di identificare gli Addetti del trattamento, nonché a formare e responsabilizzare in modo corretto tali figure.

Il Titolare si limita a raccogliere i dati strettamente necessari ad adempiere agli obblighi professionali, etici e morali derivanti dalla propria attività, conservandoli per un tempo limitato necessario a garantire la tutela della salute per i propri assistiti e ad adempiere ad eventuali obblighi di legge in materia.

Il Titolare assicura per quanto possibile la protezione dei dati fin dalla fase di progettazione della propria attività e opta per criteri di protezione per impostazione predefinita, in particolare per la tutela dei minori e dei dati particolari in suo possesso.

Il Titolare si impegna a proteggere i propri archivi in modo proporzionale alla importanza dei dati conservati e comunque a fare fronte a ogni possibile perdita di dati utilizzando gli strumenti tecnologici a disposizione in modo mirato e giustificato dal valore dei dati stessi ed all'impatto che tali dati hanno sulla libertà ed i diritti degli interessati.

Il Titolare si impegna a impiegare in modo corretto gli strumenti necessari per un moderno svolgimento del lavoro, quali PC e telefoni smartphone.

Le dotazioni saranno impiegate in modo corretto e trasparente, per i soli scopi lavorativi previsti. Saranno evitati usi impropri, così come usi potenzialmente critici per la sicurezza dei dati.

Il Titolare favorisce la cooperazione con le autorità ai fini di controllo, ove questa dovesse risultare necessaria.

Luogo e data Acquapendente
17/11/2023

Il Titolare
GEMMA MEDICA s.a.s.
di Beatrice Pelo
Via Ilaria Alpi 3
01021 Acquapendente (VT)
C.F./ P.IVA 01783800566

2. REGISTRO DEL TRATTAMENTO

Categoria dati trattati	da dove vengono presi	come sono trattati	chi è resp. del trattam.	chi è addetto al trattamento	risultato finale
Pazienti Anagrafica: nominativo, telefono, data di nascita	Colloquio con i pazienti	Conservati su archivi informatici e cartacei	Titolare	Segreteria	I dati sono utilizzati per consentire di gestire l'agenda delle visite e per favorire il contatto tra pazienti e medici
Pazienti Dati Particolari sulla salute	Esami di laboratorio Esami clinici	I dati sono resi non accessibili al personale Gemma Medica sas	Titolare Contitolare: Medico curante	Segreteria	Diagnosi mediche. I dati sono chiusi in busta sigillata, per tutelare la privacy dei pazienti. Su autorizzazione esplicita dei pazienti possono essere raccolte immagini a scopi divulgativi o promozionali
Anagrafica Medici Curanti nominativo, telefono, data di nascita, Mail	Colloquio con i medici professionisti	Conservati su archivi informatici e cartacei	Titolare	Segreteria	I dati sono utilizzati per consentire di gestire l'agenda delle visite e per favorire il contatto tra pazienti e medici
Dipendenti nominativo, telefono, data di nascita, mail, riferimenti bancari, dati sulla salute per compilare busta paga	Colloquio al momento della assunzione	Conservati su archivi informatici e cartacei	Titolare	Segreteria	I dati sono usati per gestire il rapporto di lavoro e gli oneri legali connessi
Clienti e Fornitori nominativo, telefono, data di nascita, mail, riferimenti bancari,	Al momento della stipula di un contratto, anche verbale	Conservati su archivi informatici e cartacei	Titolare	Segreteria	I dati sono usati per gestire il contratto di lavoro
Immagini videocamere	Sistema interno di videosorveglianza	Conservati su supporti informativi	Titolare	Titolare	Videosorveglianza, a scopo di tutela patrimoniale, autorizzata da INL in data 27.11.2018

3. VALUTAZIONE DI IMPATTO PRIVACY

I dati come sopra riportati e gestiti da parte del titolare del trattamento, dei contitolari, dei responsabili e degli addetti come nominati dal titolare, sono raccolti secondo i seguenti criteri:

LICEITÀ DEL TRATTAMENTO

Dati raccolti ai fini di effettuare visite mediche. Il trattamento dei dati è necessario per garantire il diritto alla salute degli interessati ed è pertanto da considerare lecito in base all'art. 6 c. 2 lett. d) del Regolamento.

Dati raccolti per finalità divulgative e promozionali: i dati sono trattati solo dopo esplicito consenso degli interessati.

CRITERI DI RACCOLTA DEL CONSENSO

Dati raccolti ai fini di effettuare visite mediche. In funzione del punto precedente, il trattamento può essere effettuato senza la raccolta del consenso degli interessati.

Dati raccolti per finalità divulgative e promozionali: il consenso è raccolto in fase di primo contatto fisico con l'interessato e comunque prima di divulgare immagini o informazioni che lo riguardino.

DIRITTI DELL'INTERESSATO

(indicare come viene concesso a l'interessato di esercitare i propri diritti)

Trasparenza delle informazioni: le informazioni raccolte vengono mediante colloquio diretto con gli interessati (medici e pazienti) e spiegando agli interessati stessi le modalità e gli scopi

Accesso alle informazioni: gli interessati possono chiedere al Titolare quali dati personali sono accolti e come sono trattati

Diritto di rettifica, cancellazione, limitazione di trattamento: gli interessati sono portati a conoscenza dei loro diritti e possono contattare il Titolare del trattamento se lo ritengono necessario, direttamente o per pec.

Diritto alla portabilità dei dati: viene garantito su richiesta il diritto alla portabilità dei dati, secondo modalità che garantiscono la privacy degli interessati

Uso o meno di processi automatizzati di decisione: non vengono impiegati sistemi automatici di decisione o di profilazione.

Diritto di opposizione: ali interessati viene garantito il diritto all'opposizione secondo le modalità indicate dalla normativa-

ESITO DELLA VALUTAZIONE

I dati trattati rappresentano un significativo rischio per i diritti e le libertà degli interessati

Le modalità di trattamento sono tali da ridurre al minimo i rischi per i diritti e le libertà degli interessati

I dati raccolti sono proporzionali rispetto a tali scopi.

I dati gestiti da GEMMA MEDICA sas. Sono **in generale esclusivamente dati anagrafici** per consentire di facilitare la gestione delle agende appuntamenti tra pazienti e medici. Sono anche passati dati clinici, ma all'interno di buste chiuse, che non sono aperte dal personale Gemma Medica sas.

I dati anagrafici vengono conservati per tutto il tempo durante il quale un interessato (paziente) indica come medico di Base un professionista che si appoggia alla struttura Gemma Medica sas. Possono essere conservati più a lungo, al solo scopo di permettere verifiche di legge o di facilitare la conservazione di dati utili per favorire il contatto tra medici curanti e i pazienti.

Eventuali immagini o altri dati relativi a prestazioni effettuate presso le strutture GEMMA MEDICA, destinati a diffusione via social o informatica o cartacea, che dovessero raffigurare persone o informazioni direttamene riconducibili a persona, sono raccolte e gestite solo dopo esplicita approvazione scritta degli interessati.

In ogni caso tutti i dati vengono distrutti dopo dieci anni dall'ultimo contatto con lo studio GEMMA MEDICA sas.

3.1 DETTAGLIO DELLA VALUTAZIONE

Il rischio è ottenuto valutando il prodotto Impatto x Probabilità. Viene costruita una matrice 3x3

Impatto: 1 basso, 2 medio, 3 alto

Probabilità: 1 bassa, 2 media, 3 alta,

da cui:

Rischio: 1-3 basso 4-6 medio 7-9 significativo o alto

Categoria dati trattati	Impatto	Probabilità	Rischio
Anagrafica Pazienti	1	2	2
Pazienti Dati Particolari sulla salute	3	1	3
Anagrafica Medici Curanti	1	2	2
Dipendenti	2	1	2
Clienti e Fornitori	1	1	1
Immagini Videocamere	1	1	1

3.2 MODALITÀ DI GESTIONE DEI DATI

I dati vengono gestiti attraverso:

- archivi informatici, conservati nei PC dello studio, tramite programma ALFADOCS, il cui accesso è consentito solo alla segreteria e al Titolare. I pazienti, gli informatori aziendali e in genere i visitatori sono filtrati in sala di attesa. Al termine della visita escono e non possono pertanto rappresentare un rischio di accesso indebito.
- I medici possono usare il PC aziendale, ma hanno accesso ad aree a loro riservate, tramite proprie password, non conosciute dal personale GEMMA MEDICA sas.
- back up locale dei dati su disco esterno (NAS) custodito direttamente dal Titolare del Trattamento, mentre il sito gestionale degli appuntamenti ALFADOCS lavora in cloud in paesi UE.
- la gestione dei dati sanitari è gestita direttamente dai medici, senza coinvolgimento aziendale. Il personale di segreteria si limita a passare le buste contenenti dati sanitari, sigillate e siglate dai medici, ai pazienti, senza poter accedere al contenuto e senza poter rompere il sigillo in modo occulto.
- Archivi cartacei per la raccolta dei consensi

3.3 RIDUZIONE DEL RISCHIO DATI

Per rendere comunque minimo il rischio di perdita o di interferenze indebite in relazione ai dati trattati, sono state prese le seguenti misure

PROTEZIONI DI TIPO INFORMATICO

- redazione di una politica della privacy riportata all'inizio del presente documento, che indica i criteri con i quali i dati sono raccolti e gestiti
- nomina formale di contitolari, responsabili del trattamento e di addetti al trattamento, se necessario
- formazione al personale interno coinvolto nel trattamento
- Informativa al personale medico esterno che collabora con lo Studio
- accesso a tutti gli strumenti informatici via password
- adozione di sistema antivirus e firewall, costantemente aggiornati in automatico
- divieto di uso dei PC di lavoro per uso personale

PROTEZIONI DI TIPO FISICO

- accesso controllato alle aree dove sono conservati archivi e dati
- adozione di sistemi di protezione antincendio adeguati (estintori, numeri di soccorso vicino a un telefono collegato con l'esterno)
- adozioni di protezioni contro le calamità naturali (si ritiene sufficiente tenere copia dei dati essenziali per il lavoro, in un disco fisso o su un'agenda cartacea, fisicamente ubicati in luoghi diversi dalla sede operativa o su cloud)

- GESTIONI DATI RACCOLTI A SCOPI DIVULGATIVI
- Nel caso di utenti che abbiano prestato consenso alla divulgazione di immagini o di dati comunque loro riconducibili, verranno prese le seguenti misure di riduzione del rischio:
- . minimizzazione dei dati personali raccolti, sia in termini di immagini, sia in termini di altri dati raccolti comunque riconducibili a persone fisiche
- . conservazione dati cartacei in archivi chiusi in area non accessibile a terzi
- . conservazione immagini su supporti informatici dedicati (es. memorie esterne), conservati in area non accessibile a terzi, rendendo irriconoscibili le persone interessate, selezionando le inquadrature in modo opportuno o utilizzando tecniche di fotoritocco (in tal caso senza conservare l'immagine originale)
- . nel caso di immagini caricate su PC le immagini saranno cancellate dal supporto originario, e il PC protetto da password ed accessibile solo a Titolare e personale autorizzato. Possibilmente la cancellazione dovrà avvenire con criteri che garantiscano l'impossibilità di recuperare l'immagine sul supporto originario (*data shredding,* funzionalità di solito ricompresa negli antivirus in commercio).
- . conservazione dei dati per non più di dieci anni.

4 CONTENUTI FORMAZIONE DEL PERSONALE

Al momento l'attività professionale è svolta direttamente dal Titolare, che si impegna ad aggiornare la propria formazione sui seguenti argomenti:

- criteri di uso di smartphone e pc impiegati per lavoro. Importanza si evitare un uso promiscuo;
- le più comuni frodi informatiche;
- compiti e responsabilità di titolari, contitolari, responsabili ed addetti del trattamento;
- cosa dice in breve il regolamento privacy;
- nuove figure previste dalla normativa;
- nuovi obblighi imposti dalla normativa;
- modalità raccolta e gestione dei consensi;
- criteri di protezione dati utili in funzione del rischio per libertà e diritti degli interessati;
- criteri di riduzione del rischio dati
- comportamento da tenere in merito a cosa fare e cosa non fare, procedure e buone pratiche.

5. REGISTRO DELLE VIOLAZIONI

Categoria dati trattati	Data Violazione	Effetti su Interessati (1)	Misure adottate
Anagrafica Pazienti			
Pazienti Dati Particolari sulla salute			
Anagrafica Medici Curanti			
Dipendenti			
Clienti e Fornitori			
Videosorveglianza			

Note: 1) indicare se: Bassi-Medi-Significativi

NOTA BENE: Se la valutazione di impatto della violazione comporta un rischio significativo per diritti e libertà degli interessati occorre effettuare una comunicazione al Garante entro 72 ore dalla violazione

5.1 Come usare il Registro delle violazioni

Il Regolamento Europeo 2016/679 regolamento europeo definisce la violazione dei dati personali (data breach) come "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" art. 4.

Un data breach o violazione dei dati non viene definito solo come un evento doloso (es. un attacco informatico, accesso abusivo), ma può essere anche un evento incidentale (es. incendio, allagamento).

La perdita di una chiavetta USB o altri dispositivi informatici e/o cartacei contenenti dati personali viene considerato una violazione di dati personali; pertanto il nuovo regolamento generale europeo prescrive specifici adempimenti nel caso di una violazione di dati personali.

Notifica della violazione

In caso di violazione dei dati il titolare dovrà notificare l'evento all'autorità di controllo.

L'art. 33 del GDPR prevede l'obbligo di notificare alle autorità di controllo la violazione dei dati, tranne che nel caso in cui "sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" (es. perdita di una chiavetta usb con dati cifrati). La notifica deve avvenire "senza ingiustificato ritardo e comunque entro 72 ore dal momento in cui ne è venuto a conoscenza"

Qualora la notifica non avvenga nelle 72 ore, il titolare dovrà indicare con giustificata motivazione, il perché del ritardo. Il GDPR prevede la possibilità di allegare ulteriori informazioni in un momento successivo, per cui è preferibile comunque effettuare la notifica nelle 72 ore, anche se è incompleta per poi predisporre idonea documentazione che verrà inoltrata.

Contenuto della notifica

La notifica deve avere il contenuto previsto dall'art. 33 del GDPR:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

- descrivere le probabili conseguenze della violazione dei dati personali;

- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

ALLEGATO

ELENCO SOGGETTI ESTERNI
TITOLARI AUTONOMI, CONTITOLARI, RESPONSABILI

SOGGETTO ESTERNO	INDIRIZZO	COMPITI	PRIVACY
			TITOLARE AUTONOMO
			TITOLARE AUTONOMO
			TITOLARE AUTONOMO
			TITOLARE AUTONOMO
			TITOLARE AUTONOMO