

## 1. Organizzazione della protezione dei dati e attribuzione delle responsabilità per la protezione dei dati

La business unit AIS (ambulatory information system) di CompuGroup Medical Italia Spa (CGM) considera la protezione dei dati personali e la loro gestione responsabile un principio cardine. CompuGroup Medical Italia spa si impegna a rispettare rigorosamente tutte le leggi e i regolamenti in vigore in materia di conservazione e trattamento dei dati personali.

La società capogruppo tedesca CGM SE ha istituito un sistema centrale di gestione della protezione dei dati che garantisce un coerente ed elevato livello di protezione dei dati personali e la conformità alle leggi sulla protezione dei dati in tutte le società del gruppo CGM.

Questa dichiarazione sulla protezione dei dati ha lo scopo di soddisfare gli obblighi di legge, fornendo informazioni sulla gestione dei dati all'interno di CGM. Questa dichiarazione sulla protezione dei dati si riferisce specificamente al prodotto CGM PHRONESIS.

In qualsiasi momento, potrete avere accesso all'ultima versione di questa dichiarazione sulla protezione dei dati sul sito prodotto di CGM PHRONESIS accessibile anche dall'interno del CGM PHRONESIS stesso.

## 2. CGM PHRONESIS

CGM PHRONESIS è un sistema di gestione degli studi medici adatto a tutte le comuni forme organizzative previste dalle convenzioni Nazionali e Regionali. Questo sistema di gestione supporta gli studi medici nel rispettare la conformità ai requisiti di legge, nel mantenimento di una documentazione strutturata, nella gestione dello studio medico, nella fatturazione, nell'emissione di ricette e in altri requisiti che possono essere soddisfatti mediante estensioni di prodotto modulari opzionali e non. CGM PHRONESIS offre una gestione dei diritti utente dedicata che limita l'accesso al software e alle estensioni software modulari alle persone autorizzate. Oltre al controllo dell'accesso al software e alle estensioni software modulari, la gestione dei diritti dell'utente controlla anche la gestione dell'accesso in lettura e scrittura ai dati memorizzati e trattati all'interno del sistema.

## 3. Trattamento dei dati personali da parte di CGM

Per dati personali si intende qualsiasi informazione relativa a una persona fisica identificata o identificabile. Una persona fisica identificabile è qualcuno che può essere identificato, direttamente o indirettamente, in particolare facendo riferimento a un elemento come un nome, un numero di identificazione, dati di localizzazione, un identificativo online o uno o più fattori specifici caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona.

Quando si utilizzano i prodotti e/o i servizi proposti, i seguenti tipi di dati vengono memorizzati da CGM sui propri server:

- **Dati contrattuali e di registrazione**
- **Dati provenienti da operazioni tecniche**

In conformità alle leggi sulla protezione dei dati, ci impegniamo a cancellare tutti i dati contrattuali, i dati di registrazione e i dati provenienti da operazioni tecniche dopo la cessazione del contratto.

Tuttavia, siamo anche obbligati dal diritto commerciale e fiscale a rispettare i periodi di conservazione obbligatoria che possono estendersi oltre la risoluzione del contratto. I dati provenienti da operazioni tecniche vengono memorizzati finché tecnicamente necessari e vengono cancellati al più tardi dopo la cessazione del contratto.

### 3.1 Dati contrattuali e di registrazione

I dati relativi al contratto e alla registrazione identificano e gestiscono il rapporto contrattuale tra studio medico e CGM. Questi dati includono:

- Dati relativi allo studio medico
  - Nome dello studio
  - Tipo di studio
  - Indirizzo dello studio
  - Codice Fiscale/Partita IVA
  - Recapiti di contatto:
    - Mail/PEC
    - Telefono/Cellulare
    - Fax
    - Indirizzo web
  - Identificativo/numero di identificazione dello studio
  - Ulteriori informazioni
- Dati relativi al medico / professionista
  - Titolo
  - Nome / cognome
  - Suffisso del nome
  - Identificativo/numero di identificazione del medico / professionista
  - Branchia specialistica
  - Ruolo professionale/Istituzionale
  - Ulteriori informazioni

Informazioni non obbligatorie che possono essere aggiunte:

- Sesso
- Data di nascita
- Nazionalità
- Numero di telefono privato
- Numero di cellulare privato
- Dati bancari (autorizzazione di addebito)
- Indirizzo e-mail privato
- Persona/e di contatto
- Appartenenza organizzativa e Ruolo
- Valutazione del cliente
- Ulteriori informazioni

La memorizzazione e il trattamento dei dati personali comunicati a CGM durante il rapporto commerciale e contrattuale servono ad adempiere al contratto e si limitano a questo scopo, in particolare per quanto riguarda il trattamento degli ordini e l'assistenza clienti.

Solo se autorizzato mediante una dichiarazione di consenso, questi dati possono essere utilizzati anche per indagini sui clienti relative al prodotto e per finalità di marketing.

I dati non potranno essere trasferiti o venduti a terzi, salvo quanto necessario per l'adempimento degli obblighi contrattuali o se espressamente autorizzato mediante una dichiarazione di consenso. A titolo esemplificativo, potrebbe essere necessario che CGM trasmetta l'indirizzo e i dati dell'ordine a un partner di vendita e assistenza quando viene effettuato un ordine. Potrebbe anche essere necessario trasmettere l'indirizzo a una società di produzione esterna allo scopo di produrre e spedire il supporto dati di aggiornamento.

I dati del contratto sono memorizzati sui server CGM SE.

Avete il diritto di essere informati sui vostri dati memorizzati, il diritto alla rettifica, il diritto alla limitazione del trattamento e il diritto alla cancellazione di questi dati.

### 3.2 Dati provenienti da operazioni tecniche

I dati provenienti da operazioni tecniche sono necessari per la fornitura dei servizi contrattualmente garantiti. CGM raccoglie dati provenienti da operazioni tecniche solo per questo scopo. CGM si accerta regolarmente

che vengano raccolti, memorizzati e trattati esclusivamente i dati necessari a fornire il prodotto e migliorarne il funzionamento.

I dati dal sistema di gestione dello studio medico vengono raccolti solo dopo la dichiarazione di consenso.

Quando si utilizzano i nostri servizi online, vengono memorizzati i dati necessari per mantenere l'integrità e la sicurezza del sistema, quali:

- Indirizzo IP del computer client
- ID computer cliente
- Durata della connessione
- Data e ora di accesso e chiusura
- Informazioni sulla trasmissione
- Sistema operativo del computer
- Serial Number dell'applicativo software
- Regione

I dati provenienti dalle operazioni tecniche sono memorizzati sui server di CGM SE e dei fornitori di connettività. I dati provenienti da operazioni tecniche vengono memorizzati finché tecnicamente necessari e vengono cancellati al più tardi dopo la cessazione del contratto.

#### **4. Trattamento dei dati personali mediante CGM PHRONESIS sul server dello studio**

- Dati anagrafici dello studio e dei suoi dipendenti
- Dati dei pazienti
  - dati anagrafici personali
  - dati sensibili

Questi dati vengono memorizzati e trattati nel database sul server dello studio.

##### **4.1 Dati anagrafici dello studio e dei suoi dipendenti**

I dati anagrafici dello studio vengono memorizzati per ragioni di conformità ai requisiti di legge e per consentire l'utilizzo corretto di alcuni moduli o contratti. Alcuni dati anagrafici vengono pertanto segnalati come obbligatori in CGM PHRONESIS. I dati anagrafici dello studio e dei suoi dipendenti comprendono:

- Nome dello studio
- Tipo di studio
- Indirizzo dello studio
- Identificativo/numero di identificazione dello studio
- Specialità medica
- Dati relativi al medico / professionista
  - Titolo
  - Nome / cognome
  - Identificativo/numero di identificazione del medico / professionista
  - Ulteriori informazioni
- Altri dipendenti dello studio
  - Cognome
  - Nome
  - Nome utente / password
  - Ulteriori informazioni

I dati anagrafici sono necessari quando si utilizzano diversi moduli software per eseguire azioni e vengono utilizzati automaticamente. La trasmissione a terzi viene effettuata previa dichiarazione di consenso o interazione dell'utente. La rettifica, la restrizione del trattamento o la cancellazione di questi dati è possibile ma può essere limitata dai requisiti di legge. Le descrizioni relative alla rettifica, alla restrizione del trattamento o alla cancellazione dei dati sono disponibili nella documentazione di prodotto periodicamente distribuita.

##### **4.2 Dati del paziente**

L'archiviazione, l'utilizzo e il trattamento dei dati del paziente sono ammessi solo con il consenso del paziente stesso (soggetto interessato) o sulla base di un obbligo di legge. I dati del paziente non vengono generati automaticamente in CGM PHRONESIS. I dati del paziente vengono raccolti e inseriti in CGM PHRONESIS dallo studio rispettivamente dal medico o dal personale che lavora presso lo studio medico.

**Dati anagrafici del paziente:** i dati anagrafici del paziente possono essere acquisiti e inseriti automaticamente mediante procedure elettroniche o moduli software (ad es. servizi regionali e/o nazionali) e/o inseriti o completati da inserimento manuale dei dati.

Alcuni dati anagrafici vengono segnalati come obbligatori in CGM PHRONESIS

perché necessari per l'adempimento degli obblighi contrattuali o legali.

Le informazioni obbligatorie comprendono solo le informazioni personali quali:

- Nome
- Cognome
- Prefisso o suffisso
- Data di nascita
- Sesso

I dati aggiuntivi non obbligatori includono:

- Indirizzo (via, numero civico, codice postale, città, paese)
- In caso di riferimento ad altri, informazioni quali
  - Medico di riferimento
  - Tutori o persone di riferimento
- Foto del paziente (necessaria la dichiarazione di consenso)
- Numero di telefono privato
- Numero di cellulare
- Indirizzo e-mail

**Dati sensibili:** i dati sanitari sono una categoria speciale di dati personali e sono soggetti a una maggiore tutela dalla normativa sulla protezione dei dati.

L'integrazione dei dati nella cartella clinica del paziente deriva dall'obbligo legale del medico curante di documentare tutte le misure e i relativi risultati rilevanti per il trattamento attuale e futuro del paziente.

Questi dati includono:

- Anagrafe sanitaria
  - Esenzioni per status e patologia
- Anamnesi e abitudini di vita
- Diagnosi
- Accertamenti diagnostici
- Risultati degli accertamenti diagnostici
- Esiti
- Terapie e loro rispettivi risultati
- Interventi e loro rispettivi risultati
- Documentazione e informazioni sul consenso
- Lettere al collega
- Statistiche sanitarie
- Prescrizioni
  - Farmaceutiche
  - Parafarmaceutiche
  - Omeopatici
  - Richieste e accertamenti
  - Ricoveri
- Diete

Sono possibili accessi, modifiche e cancellazioni della cartella clinica del paziente a cura del Titolare del trattamento o dei suoi incaricati. L'esportazione dei dati è possibile (portabilità dei dati) in un formato strutturato e leggibile anche da dispositivo automatico, il file può essere trasmesso al paziente su richiesta. Le procedure e le funzionalità

corrispondenti sono disponibili nella documentazione di prodotto periodicamente distribuita.

#### **4.3 Trattamento di dati dello studio e di dati personali sensibili e dei dati del paziente in moduli software**

I moduli integrati possono essere installati e attivati in associazione a CGM PHRONESIS con cui interagiscono e partecipano al trattamento dei dati personali.

Moduli integrati:

- Add-On Regionale integrazione ai servizi Regionali Sanitari (Prescrizione dematerializzate, FSE, PIPP, ADI/ADP, certificati INPS, ecc.)
- Moduli e procedure di elaborazione dati (opzionali) per ottemperare ai debiti informativi nei confronti di sistemi e servizi Nazionali e Regionali
- CGM drCLOUD (opzionale) per la gestione dei dati sanitari sincronizzati sui vari dispositivi (cellulari, tablet, desktop)

#### **5. Trasmissione / trasferimento dei dati**

Il trasferimento elettronico dei dati basato sul consenso legale, contrattuale o preventivo viene effettuato da CGM PHRONESIS solo dopo l'interazione con l'utente o automaticamente, se ciò è stato autorizzato.

CGM PHRONESIS unitamente all'utilizzo dei moduli integrati consente di trasferire i dati sanitari e personali agli attori istituzionali, sistemi e servizi informatici Nazionali e Regionali in conformità delle specifiche tecniche di riferimento e delle norme e protocolli indicati.

E' possibile che dati e contenuti siano resi disponibili attraverso attori istituzionali e sistemi terzi con altri medici in associazioni e/o dipendenti.

Alcune informazioni potrebbero essere trasferite per ottemperare a specifici obblighi contrattuali in ambito di Convezione SSN.

L'utente garantisce di aver ottenuto tutti i permessi, i consensi, le informative e le autorizzazioni comunque necessarie, prima di inviare, condividere e/o comunicare dati e contenuti.

#### **6. Obblighi di riservatezza, formazione sulla protezione dei dati**

Come ulteriore misura atta a garantire un'adeguata sicurezza dei dati personali, tutti i nostri dipendenti hanno sottoscritto un idoneo accordo di riservatezza, sono stati opportunamente autorizzati al trattamento dei dati da parte di CGM ed hanno ricevuto precise istruzioni in merito. L'accesso alle informazioni sensibili da parte dei nostri incaricati può avvenire solo per ragioni legate alla fornitura dei servizi, assistenza, risoluzione guasti o completamento di attività espressamente richieste.

CGM ha introdotto misure e processi per applicare le regole sulla privacy e sulla protezione dei dati a tutti i collaboratori fornendo una formazione continuativa in materia di riservatezza e protezione dei dati.

#### **7. Misure di sicurezza / prevenzione del rischio**

CGM adotta tutte le necessarie misure di sicurezza tecniche e organizzative per proteggere i vostri dati personali e quelli dei vostri pazienti da accessi non autorizzati, alterazioni, divulgazione, perdita, distruzione e altre forme di abuso. Queste misure comprendono analisi interne e verifiche dei nostri processi di raccolta, archiviazione e trattamento dei dati, nonché misure di sicurezza per proteggere i sistemi IT, su cui archiviamo dati contrattuali e dati provenienti da operazioni tecniche, da accessi non autorizzati.

#### **8. Misure tecniche e organizzative**

Per garantire la sicurezza dei dati, CGM rivede regolarmente lo stato dell'arte delle tecnologie di sicurezza. Ciò include la determinazione di scenari di danno tipici, le esigenze di sicurezza e i livelli di sicurezza corrispondenti che ne derivano per diversi tipi di dati personali, raggruppati in categorie di possibili danni, nonché l'esecuzione di valutazioni del rischio.

Inoltre, vengono effettuati test di penetrazione dedicati per analizzare, esaminare e valutare regolarmente l'efficacia di queste misure tecniche e organizzative che devono garantire la sicurezza del trattamento.

I seguenti orientamenti disciplinano l'attuazione di misure tecniche e organizzative appropriate:

- **Backup dei dati (servizi SaaS)**

Per evitare perdite, i dati vengono regolarmente sottoposti a backup veicolate dalle procedure di sicurezza IT di CGM SE.

- **"Privacy by design"**

CGM garantisce che i principi di protezione / privacy dei dati e di sicurezza dei dati siano presi in considerazione durante i processi di progettazione e sviluppo dei sistemi IT.

L'obiettivo è quello di prevenire un'attività di programmazione aggiuntiva, dispendiosa in termini di costi e di tempo, che sarebbe necessaria se i requisiti di privacy e sicurezza dei dati dovessero essere attuati dopo l'installazione dei sistemi IT. All'inizio del processo di sviluppo vengono prese in considerazione misure come la disattivazione di alcune funzionalità software, l'autenticazione o la crittografia.

- **"Privacy by default"**

I prodotti CGM sono dotati di impostazioni di fabbrica ottimizzate per la privacy dei dati, in modo che vengano trattati solo i dati personali necessari per il relativo scopo.

- **Comunicazione via e-mail (studio / CGM)**

Nel caso in cui si desideri contattare CGM tramite e-mail, tenere presente che la privacy delle informazioni trasmesse non può essere garantita, poiché il contenuto delle e-mail può essere visualizzato anche da terzi. Si consiglia di utilizzare il servizio postale ogni volta che si desidera trasmettere informazioni riservate.

• **Amministrazione da remoto**

Dipendenti o subappaltatori di CGM potrebbero dover accedere ai dati dei pazienti o dei clienti e occasionalmente ai dati dello studio. Tale accesso è disciplinato dalle regole generali di CGM.

- L'accesso all'amministrazione da remoto è chiuso per impostazione predefinita e viene autorizzato solo dai clienti.
- Le password per accedere ai sistemi IT dei clienti vengono rilasciate solo per finalità di amministrazione da remoto.
- Gli interventi critici sono garantiti da una procedura "4-eyes" (principio del doppio controllo) con ulteriore presenza dell'interessato.
- Utilizziamo strumenti di amministrazione da remoto richiedendo al cliente di concedere attivamente l'accesso e consentendogli di monitorare gli interventi.
- L'accesso all'amministrazione da remoto viene registrato nel sistema CRM. Vengono registrati i seguenti dati: persona responsabile, data e ora, durata, sistema di destinazione, strumento di amministrazione da remoto, breve descrizione dell'attività svolta e, in caso di interventi critici, i nominativi del personale qualificato aggiuntivo consultato nell'applicazione della procedura "4-eyes".
- La registrazione delle sessioni di amministrazione da remoto è vietata.

**9. Diritti del soggetto interessato**

**Dati personali del professionista e degli impiegati dello studio**

Avete il diritto di essere informati sui dati memorizzati che vi riguardano e il diritto di accedere a questi dati, avete il diritto alla rettifica, cancellazione, limitazione del trattamento, portabilità dei dati e il diritto di opporvi al trattamento dei vostri dati personali.

Avete il diritto di revocare il vostro consenso in qualsiasi momento. La revoca ha effetto da quel momento.

Avete il diritto di presentare un reclamo all'autorità di controllo responsabile se pensate che stiamo trattando i vostri dati in modo inappropriato.

Ci impegniamo a cancellare tutti i dati contrattuali, i dati di registrazione e tutti i dati provenienti da operazioni tecniche dopo la cessazione del contratto senza la vostra preventiva richiesta.

Siamo tuttavia obbligati dalla legislazione in materia commerciale e fiscale a rispettare i periodi di conservazione legale, che possono estendersi oltre la cessazione del contratto. I dati provenienti da operazioni tecniche restano memorizzati solo fino a quando tecnicamente necessario e vengono cancellati al più tardi dopo la cessazione del contratto.

**Dati personali del paziente**

I pazienti hanno il diritto di essere informati sui dati memorizzati che li riguardano, nonché il diritto di ricevere e trasmettere i loro dati personali (portabilità dei dati) e diritto alla rettifica, cancellazione, limitazione del trattamento e diritto di opporsi al trattamento dei loro dati personali.

Quando si ricevono richieste di cancellazione da parte di pazienti, si ha tuttavia l'obbligo di rispettare i periodi di conservazione applicabili.

I pazienti hanno il diritto di revocare il loro consenso in qualsiasi momento e la revoca ha effetto da quel momento.

I pazienti hanno il diritto di presentare un reclamo all'autorità di controllo responsabile se pensano che stiate trattando i loro dati in modo inappropriato.

**10. Applicazione**

Il rispetto delle regole sulla protezione dei dati qui descritte viene verificato regolarmente e continuamente da CGM.

Se CGM riceve una denuncia formale, la società contatterà il querelante al fine di risolvere eventuali dubbi relativi al trattamento dei propri dati personali.

CGM si impegna a collaborare con l'amministrazione competente, compresa l'autorità di controllo.

**11. Modifiche alla presente dichiarazione sulla protezione dei dati**

Si precisa che questa dichiarazione sulla protezione dei dati potrebbe essere soggetta a modifiche e integrazioni. In caso di modifiche sostanziali, pubblicheremo una comunicazione dettagliata. Ogni versione di questa dichiarazione sulla protezione dei dati può essere identificata dalla data e dal numero di versione nel piè di pagina del testo della dichiarazione stessa. Inoltre, tutte le precedenti versioni di questa dichiarazione sono archiviate e rese disponibili su richiesta del Responsabile della protezione dei dati.

**12. Responsabile per la CompuGroup Medical Italia spa**

Alessandro Avezza  
Via Adriano Olivetti, 10  
70056 Molfetta (BA)

**Responsabile della protezione dei dati**

Si prega di contattare il Responsabile della protezione dei dati per qualsiasi domanda relativa al trattamento dei vostri dati personali e per la ricezione delle vostre richieste di informazioni o reclami.

[dpo.it@cgm.com](mailto:dpo.it@cgm.com)

**13. Autorità di controllo competente**

L'autorità di controllo competente per CompuGroup Medical Italia spa è:

Garante per la protezione dei dati personali  
Piazza Venezia n. 11  
00187 ROMA  
Centralino telefonico: (+39) 06.69671  
E-mail: [protocollo@gpdp.it](mailto:protocollo@gpdp.it)  
PEC: [protocollo@pec.gpdp.it](mailto:protocollo@pec.gpdp.it)