SECURITY LAB
sicurezza on line

Panoramica per la compliance al GDPR di uno studio medico

---

1. Condivisione e Trattamento dei Dati

Per le associazioni dei medici di base, è fondamentale:

- **Condivisione dei dati**: Verificare il server o il cloud comune utilizzato dall'associazione e controllare le difese perimetrali della rete locale (LAN).
- **Personale di segreteria**: Se il personale di segreteria è fornito da un ente terzo, essi devono essere considerati **responsabili esterni del trattamento**. Lo stesso vale per infermieri, OSS e altri collaboratori non direttamente dipendenti.
- **Dispositivi personali**: Spesso medici e personale utilizzano PC, tablet o dispositivi personali collegati al gestionale. È importante verificare che rispettino le misure di sicurezza (antivirus, procedure di backup).

2. Dispositivi e Macchinari

- **Sistemi operativi**: Controllare che i sistemi operativi utilizzati siano aggiornati e dotati di misure minime di sicurezza.
- **Macchinari con memoria interna**: Dispositivi come ecografi, se conservano dati, devono essere censiti. Se non conservano dati, questa operazione non è necessaria.

3. Medici Associati e Software

- **Medici associati**: Operano come **responsabili interni del trattamento** in quanto parte dello studio.
- **Software aggiuntivi**: Ogni software o app utilizzata per la gestione delle cartelle cliniche, appuntamenti o dati sensibili deve essere censito, anche se utilizzato solo da un medico dello studio.

---

4. Nomina del DPO (Data Protection Officer)

La nomina del DPO è obbligatoria quando si tratta di dati **su larga scala**.

- **Criteri per la larga scala** (European Data Protection Board):
  - Numero di interessati, volume e tipologia dei dati.
  - Durata e ambito geografico del trattamento.
- Per associazioni di rete e aggregazioni territoriali, il numero di pazienti gestiti (es. 7500 pazienti per 5 medici) rende necessaria questa nomina.

---

5. Adempimenti GDPR Essenziali

Struttura e Organizzazione

1. **Mappatura dei dati**: Identificare i dati trattati e la loro base giuridica (es. consenso esplicito o obblighi di legge).
2. **Documentazione**:

- **Registro delle attività di trattamento**: Indicare tipologie di dati, finalità, tempi di conservazione e misure di sicurezza.
- **Informativa sulla privacy**: Redatta in modo chiaro e fornita ai pazienti.

Sicurezza dei Dati

1. Misure tecniche:
   - Backup regolari, antivirus, firewall, crittografia.
2. Misure organizzative:
   - Limitare l'accesso ai dati al personale autorizzato.
   - Predisporre un piano per notificare eventuali violazioni (data breach).

---

6. Requisiti dell'Informativa sulla Privacy

L'informativa deve essere:

- **Chiara e Trasparente**: Senza tecnicismi inutili.
- **Completa**: Deve includere:
  - Identità del titolare del trattamento.
  - Finalità e base giuridica del trattamento.
  - Destinatari dei dati, tempi di conservazione, diritti degli interessati.
  - Modalità di trattamento (es. elettronico o cartaceo).

Queste indicazioni coprono gli aspetti principali, ma è sempre consigliabile rivolgersi a un consulente esperto per personalizzare le misure in base alle specificità dello studio.