

Vademecum per i medici

Il presente vademecum è stato redatto nel rispetto delle previsioni normative di cui al “Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE” e del Decreto Legislativo 16 del 2003, c.d. “Codice privacy”.

- Il primo obbligo a carico del medico, indipendentemente dalle dimensioni del proprio studio professionale, è quello di informare il paziente circa le finalità in ragione delle quali sono raccolti i dati e circa le modalità di trattamento e conservazione dei dati stessi (vedi all.);
- In caso di studio medico condiviso, indicare nell’informativa i nominativi di altri eventuali responsabili o incaricati del trattamento;
- In relazione alla conservazione dei dati:

se i dati sono conservati su supporto cartaceo, occorre garantirne l’accessibilità riservata (es.: la segretaria dello studio medico potrà avere libero accesso ai recapiti del paziente, non certo a quelli concernenti le condizioni di salute dello stesso; del pari, le comunicazioni telefoniche con i pazienti debbono essere effettuate in maniera che non possano essere ascoltate da soggetti terzi, estranei al rapporto; sarebbe opportuno, pertanto, che la postazione telefonica della segreteria non sia ospitata nella sala d’attesa dello studio medico).

In caso di database informatico: i files non debbono essere liberamente accessibili dal PC, in ipotesi di rete di condivisione; sarebbe opportuno procedere ad una pseudonimizzazione dei dati stessi (ricollegandoli al nominativo del paziente solo tramite una chiave di garanzia, o un codice identificativo che non sia, a sua volta, un dato personale del paziente).

In relazione all'eventuale esistenza di una rete informatica o di un dispositivo di connessione internet wi-fi: si consiglia vivamente di modificare l'originaria chiave di accesso fornita dal gestore della rete e di modificarla ogni tre mesi; si consiglia di predisporre una password sui terminali mediante i quali è possibile accedere ai dati dei pazienti, benché oggetto di pseudonimizzazione, nonché di cambiarla ogni tre mesi.

Nelle non infrequenti ipotesi di condivisione degli studi medici da parte di più professionisti: occorre rispettare gli standards minimi di sicurezza, quali – a titolo meramente esemplificativo:

- Chiamare la singola visita in forma anonima (attraverso un numero);
- Rispettare la distanza di cortesia (il desk della segreteria, in ipotesi di più segretarie, non deve chiamare in contemporanea più pazienti di dottori diversi);
- Consegnare le singole prescrizioni in busta chiusa e anonima, e solo al diretto interessato (o ad altra persona, dallo stesso previamente e formalmente autorizzata al ritiro);
- Vivamente sconsigliata la comunicazione delle prescrizioni ai pazienti via mail;
- in caso di invio via mail: le ricette devono essere criptate; il paziente deve aver rilasciato previamente il consenso informato; deve essere utilizzata la posta elettronica certificata (PEC).

In relazione alla possibilità di installazione di telecamere a fini di videosorveglianza: l'eventuale controllo di ambienti sanitari, stante la natura sensibile di molti dati che possono essere in tal modo raccolti, devono essere limitati ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute e della dignità degli interessati.

Il consenso

Prima di esprimere il proprio consenso l'interessato deve essere compiutamente informato delle modalità e delle finalità di trattamento dei dati.

Il consenso deve quindi essere espresso in modo:

- Libero
- Inequivoco
- Specifico

Sono escluse forme di consenso tacito o mediante opzioni già preselezionate.

- Il GDPR non prevede obbligatoriamente la forma scritta per il consenso; purtuttavia la forma scritta è opportuna e raccomandata.
- Il consenso raccolto prima del 25 maggio 2018 resta valido se ha tutti i requisiti indicati nel Regolamento. In caso contrario, è opportuno raccogliere nuovamente il consenso.

L'informativa

L'informativa del medico dovrà fornire con linguaggio semplice e chiaro le informazioni relative al trattamento dei dati in forma concisa, trasparente, intellegibile e facilmente accessibile

Se le finalità mutano si dovrà, pertanto, acquisire un nuovo consenso.

Adempimenti del medico

In attuazione del Regolamento e al fine di garantire il rispetto dei principi in tema di trattamento dei dati personali acquisiti il medico deve:

- Predisporre il documento (c.d. registro – art. 30);

Elaborare:

- il servizio per la tutela della privacy con definizione ex ante delle singole fasi;
- il servizio per il trattamento dei dati;
- il servizio con le procedure di sicurezza;
- il servizio per le verifiche di tenuta del sistema (che comprende la necessità di adeguamento degli strumenti informatici) e le responsabilità.
- Consegnare ai propri pazienti l'informativa (**vedi all.**) (con ricevuta a firma dell'interessato per presa visione).