# 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" (d'ora innanzi, *breviter*, "GDPR" o "Regolamento") e del Decreto Legislativo 16 del 2003, c.d. "Codice privacy".

La maggior parte degli obblighi previsti dal Regolamento, d'implementazione del sistema normativo concernente il trattamento dei dati personali, non si applica al professionista sanitario.

Il presente vuol essere, nelle intenzioni, un documento di sintesi, con l'elencazione di una serie di suggerimenti (alcuni oggetto di obbligo normativo; altri dettati dal semplice buonsenso) utili al singolo medico per garantire fattivamente la sicurezza dei dati personali trattati.

*******

Il medico di base si trova, nella quotidiana attività professionale, a dover trattare dei dati personali di una certa delicatezza, quali quelli genetici (i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione(art. 4 n. 13 GDPR); i dati biometrici (i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (art. 4 n. 14 GDPR); quelli relativi alla salute (i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4 n. 15 GDPR).

Il trattamento è disciplinato sotto un duplice profilo:

- Informativa e consenso nella acquisizione dei dati personali.
- Utilizzo e circolazione dei dati stessi.

Il GDPR si fonda sul principio della c.d. *"accountability"*: essa è la responsabilità del titolare del trattamento cui compete garantire l'efficacia della tutela predisposta, ricomprendente il riesame e l'aggiornamento costante di tutte le condizioni adottate.

**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.** Si allega al presente documento un facsimile di **informativa**.

Si sottolinea come sia opportuno, in caso di studio medico condiviso, indicare nell'informativa i nominativi di altri eventuali responsabili o incaricati del trattamento (es.: i c.d. "sostituti").

A seguito della comunicazione e della sottoscrizione dell'informativa, il paziente potrà prestare formalmente il proprio consenso informato. Si allega al presente documento un facsimile di **lettera di prestazione del consenso.**

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 pseudonmizzazione 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 medianti 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: l'art. 1, comma 4, decreto del MEF del 2 novembre 2011 prevede infatti che *"il medico prescrittore rilascia all'assistito il promemoria cartaceo della ricetta elettronica secondo il modello riportato nel disciplinare tecnico Allegato 2"*. Il menzionato decreto, precisa che potranno essere resi disponibili ulteriori canali per accedere ai servizi di cui al presente disciplinare erogati dal Sac, in modo particolare per la fruizione del promemoria da parte degli assistiti (art. 3.5.1.) attraverso il sito del Ministero dell'economia e delle finanze (www.sistemats.it) (art. 4.1.). Ma allo stato le modalità alternative per usufruire del promemoria non sono state ancora individuate. Pertanto, il Garante ha specificato che nell'attesa che il MEF stabilisca le vie alternative per l'invio del promemoria cartaceo la posta elettronica è a rischio sanzioni per violazioni della Privacy. Conseguentemente, 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 (o, addirittura, il monitoraggio di pazienti ricoverati in particolari reparti o ambienti), 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. Naturalmente, le immagini idonee a rivelare lo stato di salute delle persone non devono essere comunque diffuse, per cui va assolutamente evitato il rischio di diffusione delle immagini di persone malate su monitor collocati in locali liberamente accessibili al pubblico.

**I dati raccolti dal medico devono essere:**

- **Finalizzati:** strettamente pertinenti a quanto necessario per lo scopo del trattamento dichiarato. Conseguentemente, l'informazione espressa da parte del medico delle finalità in funzione delle quali il consenso del paziente è espresso deve precedere l'acquisizione del consenso affinché quest'ultimo sia effettivamente consapevole.
- **Accurati:** occorre verificarne la correttezza, la veridicità e la completezza. Conseguentemente, il medico è tenuto non solo a trattare dati esatti garantendone la qualità; il medico deve anche approntare un'organizzazione che garantisca il relativo controllo, con adozione di tutte le misure necessarie alla rettificazione o cancellazione di dati inesatti.
- **Limitati:** quantitativamente determinati a quanto strettamente necessario alle finalità dichiarate nell'informativa.
- **Utilizzati**: in modo riservato e confidenziale: il medico deve garantirne la sicurezza attraverso l'utilizzo di sistemi di sicurezza (ad esempio: attraverso la cifratura dei dati: associando il dato personale relativo allo stato di salute di un assistito non direttamente al suo nominativo, ma ad un codice in base al quale individuare solo in maniera indiretta – attraverso l'accesso ad una banca dei nomi dei pazienti "cifrati", banca dei nomi a sua volta garantita da password se telematica o da forme di sicurezza "materiali" se fisica.
- **Conservati** ed archiviati non oltre il tempo strettamente necessario: il tempo necessario è quello indispensabile alle finalità del trattamento.

**Il trattamento.** Il trattamento deve avvenire in maniera:

- **Lecita:** deve fondarsi sul consenso dell'interessato o su altra base giuridica. Il trattamento è considerato sempre lecito se necessario all'adempimento di un obbligo legale.
- **Corretta:** nel rispetto dell'informazione resa all'interessato in relazione alla raccolta, all'utilizzo e ad altri successivi trattamenti dei dati forniti.
- **Trasparente:** deve essere realizzato con modalità predefinite e rese note all'interessato in maniera chiara, semplice ed accessibile, anche in relazione alla "forma" utilizzata. Pertanto, è da escludersi l'utilizzazione, in àmbito medico, di una terminologia eccessivamente tecnica.

**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 (deve, pertanto, riferirsi ad un preciso trattamento e non può essere generico ed estendibile a vari possibili trattamenti).

**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, in quanto l'art. 7 GDPR onera il titolare del trattamento di *"di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali"*.
- 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.
- *"Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma*

*comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro"* (art. 7, § 2 GDPR).

**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 e dovrà contenere:

- i riferimenti di contatto del medico (recapiti: telefono; fax; indirizzo di posta elettronica) per le comunicazioni relative all'esercizio dei diritti.
- La precisa e dettagliata descrizione delle finalità per cui viene posto in essere il trattamento.
- La specifica e chiara indicazione dei diritti di revoca del consenso, di accesso ai dati, di rettifica, di cancellazione, di limitazione del trattamento, di portabilità dei dati e di opposizione.

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