Privacy: vademecum per il medico di famiglia

Il Garante per la protezione dei dati personali ha approvato in via definitiva le "Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario" (G.U. n. 178 del 3 agosto 2009). Le "Linee guida", adottate al termine di una consultazione pubblica con gli operatori del settore, fissano un primo quadro di regole a protezione dei dati sanitari e integrano la normativa sulla privacy in attesa di una legislazione ad hoc sull'argomento.

Gianluca Bruttomesso

Il provvedimento approvato dal Garante della privacy in tema di fascicolo sanitario elettronico (Fse) detta regole che ampiano il quadro della legge in materia di tutela dei dati personali. In particolare tale provvedimento stabilisce che il paziente deve poter scegliere, in piena libertà, se far costituire o meno un fascicolo sanitario elettronico, con tutte o solo alcune delle informazioni sanitarie che lo riguardano; deve poter manifestare un consenso autonomo e specifico, distinto da quello che si presta a fini di cura della salute; al paziente deve essere inoltre garantita la possibilità di "oscurare" la visibilità di alcuni eventi clinici.
Per poter esprimere scelte consapevoli il paziente deve essere adeguatamente informato. Con un linguaggio comprensibile e dettagliato, l'informativa deve quindi indicare chi (medici di famiglia, del reparto ove è ricoverato l'assistito, farmacisti) ha accesso ai suoi dati e che tipo di operazioni può compiere.
Il fascicolo sanitario elettronico potrà essere consultato dal paziente con modalità adeguate (per esempio, tramite smart card) e dal personale sanitario strettamente autorizzato, solo per finalità sanitarie. Non potranno accedervi invece periti, compagnie di assicurazione, datori di lavoro.
In ogni caso se il paziente non vuole aderire al Fse deve comunque poter usufruire delle prestazioni del servizio sanitario nazionale.
Gli accessi alle informazioni infine, dovranno essere tracciabili e graduali, e i dati sanitari dovranno essere protetti con misure di sicurezza molto elevate che limitino il più possibile i rischi di abusi, furti, smarrimento.
Entro il 31 dicembre Regioni e Asl dovranno comunicare al Garante della privacy le iniziative già avviate sul fascicolo sanitario elettronico e d'ora in poi ogni iniziativa che riguarda il Fse dovrà sempre essere comunicata all'Autorità prima del suo avvio.

Consigli pratici

Partendo da queste linee guida è il caso di soffermarsi su alcuni punti inerenti all'attività dei medici in rapporto alle norme che regolano la privacy. Per ciò che riguarda il consenso al trattamento dei dati dei pazienti, per esempio è necessario che questo venga raccolto nell'apertura della scheda sanitaria e che la relativa informativa venga affissa in sala d'aspetto, in particolar modo nelle vicinanze dei punti di accoglienza. Tale consenso può essere raccolto anche in forma verbale, ma si consiglia di effettuare questa prassi solo in casi particolari e di non adottarla come consuetudine di lavoro.
Secondo il Garante, il personale deve essere istruito a evitare di conversare con i pazienti del loro stato di salute e in particolare delle loro patologie. La prenotazione e le visite devono avvenire con modalità tali da impedire che altri pazienti possano sentire le conversazioni e/o individuare l'interlocutore.
In presenza di altri malati o di terzi in sala d'attesa, l'operatore sanitario deve usare l'accortezza di non comunicare all'accettazione gli esiti o la necessità di eventuali altri esami a voce alta e per nessun motivo dovranno essere comunicate patologie telefonicamente.
Il Garante ha più volte sanzionato i medici di medicina generale che abbandonavano le ricette dei pazienti in ambulatorio e nelle sale d'attesa o le consegnavano a persone non autorizzate. È importante, quindi, seguire alcune semplici regole per evitare di incorrere in gravi sanzioni e/o peggio in contestazioni da parte dei pazienti. Le ricette devono essere inserite in buste chiuse e sigillate, non lasciate in sala d'aspetto, e consegnate in orari prestabiliti per il ritiro (per esempio, apertura ambulatorio, chiusura ambulatorio).

La sicurezza dei dati

Nel caso di trattamento dei dati sensibili e/o giudiziari effettuato mediante computer, deve essere predisposto e aggiornato un documento programmatico sulla sicurezza dei dati con cadenza annuale, per definire, sulla base dell'analisi dei rischi, la distribuzione dei compiti e le responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi.
L'efficacia delle misure di sicurezza deve essere sottoposta a controlli periodici, da eseguirsi con cadenza almeno annuale. Nel caso di trattamento dei dati sensibili e/o giudiziari, il reimpiego dei supporti di memorizzazione già utilizzati per il

trattamento può essere effettuato qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti. La procedura deve essere svolta entro il 31 marzo di ogni anno. Tale provvedimento è considerato dalla legge una "misura minima di sicurezza", e integra oltre che un possibile profilo di responsabilità civile nel caso di perdita e/o uso non conforme di dati con danneggiamento di terzi, un reato penalmente sanzionato dall'art. 169. Tale procedura quindi deve essere considerata un momento importante per analizzare con attenzione le misure di sicurezza e i sistemi che sono adottati per proteggere i dati dei pazienti che costituiscono un valore inestimabile; la loro perdita vorrebbe dire ricostruire archivi e perdere informazioni. Cosa bisogna fare per evitarlo? Innanzitutto è necessario cambiare la propria password almeno ogni tre mesi, formata da numeri e lettere con non meno di otto caratteri, e, per riservatezza, è opportuno non attaccare *post it* su monitor o in luoghi accessibili a terzi dove siano scritte le password. Per maggiore sicurezza è conveniente tenere copie dei dati in un luogo diverso da quello dove è situato il personal computer e fare dei regolari e giornalieri back up dei dati stessi.
Il sistema va continuamente protetto, a tale scopo va utilizzato un antivirus e firewall e un programma antispyware, poiché, anche se non collegati alla rete, i virus possono essere annidati in file contenuti in altri documenti.
Per quanto riguarda la manutenzione è bene avvalersi di personale specializzato, sottoscrivendo un contratto che obblighi il consulente al rispetto delle normative e delle più scrupolose regole di gestione.

Utilizzo di strumenti diversi da quelli elettronici

Nel caso di trattamento di dati personali effettuato con strumenti diversi da quelli elettronici o comunque automatizzati, è necessario osservare alcune procedure. Il titolare o il responsabile, nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni, deve prescrivere l'accesso ai dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato definendo procedure di consegna e restituzione dei documenti. Nel caso di trattamento di dati sensibili e/o giudiziari devono essere osservate due regole fondamentali: gli atti e i documenti contenenti i dati si devono conservare in luoghi chiusi, in contenitori muniti di serratura, l'accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.

La lettera d'incarico

La lettera d'incarico è obbligatoria. È un sistema per obbligare i terzi alla massima serietà. Il medico dovrà responsabilizzare il personale e altri collaboratori, come i suoi sostituti. In tale lettera sono specificati i compiti da rispettare al fine di garantire l'adempimento di tutti gli obblighi della legge. Deve, dunque, contenere in maniera chiara e inequivocabile informazioni e istruzioni necessarie all'assolvimento dei compiti assegnati: il trattamento dei dati deve essere effettuato in modo lecito e corretto, e per ogni operazione del trattamento deve essere garantita la massima riservatezza. Nel caso di modifica dell'incarico o di cessazione del rapporto di lavoro, gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dei dati dovranno comunque continuare ad essere riservati.
La lettera d'incarico dell'amministratore del sistema invece deve contenere una dichiarazione dello stesso di essere a conoscenza di quanto prevede il regolamento per ciò che concerne i suoi obblighi, e di rispettare le indicazioni sulla sicurezza dei dati applicate presso lo studio medico. Si deve impegnare, inoltre, ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte nonché dalle eventuali successive normative in materia. L'amministratore del sistema ha il compito di prendere tutti i provvedimenti necessari a evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back up di *disaster recovery* secondo i criteri stabiliti dal "Responsabile del trattamento per la sicurezza dei dati". L'incaricato, inoltre, deve assicurarsi della qualità delle copie di back up dei dati e della loro conservazione in luogo adatto e sicuro e provvedere affinché sia prevista la disattivazione dei "codici identificativi personali" (username, Id) nel caso di perdita della qualità che consentiva all'utente o all'incaricato l'accesso all'elaboratore, oppure, nel caso di mancato utilizzo dei codici identificativi per oltre sei mesi.
L'amministratore del sistema ha inoltre l'onere di proteggere gli elaboratori dal rischio di intrusione e dal rischio di virus mediante l'adozione di programmi idonei.

La formazione del personale

Il personale deve essere indirizzato alla corretta gestione e manutenzione dei sistemi informatici. Spesso anche il lavoratore più efficiente può utilizzare internet e la posta elettronica anche per ragioni personali. È opportuno, quindi, che oltre alla lettera di incarico sia fornita un'adeguata nota di istruzioni in modo che sia possibile procedere disciplinarmente in caso di violazioni. È importante provvedere con adeguate istruzioni scritte. Il regolamento del personale, valido ed efficace anche ai fini disciplinari ai sensi dell'art. 7 della legge 30/05/1970 n. 300, riguarda le modalità di utilizzo degli strumenti informatici nell'ambito dello svolgimento delle proprie mansioni, dei propri compiti di lavoro e nelle attività di ufficio da parte dei dipendenti che hanno in dotazione una stazione di lavoro di tipo personal computer o terminale.