Il Garante è di recente intervenuto con il provvedimento n. 55 del 7 marzo 2019 per fornire chiarimenti sulla disciplina applicabile al trattamento di dati sanitari. Il provvedimento risponde all'esigenza di dare un'interpretazione uniforme a vantaggio degli operatori e tutelare più efficacemente il paziente e i suoi dati.
Occorre anzitutto ricordare che il trattamento di dati personali è, in via generale, vietato se rivolto a rivelare lo stato di salute di un soggetto, ma il trattamento di dati particolari, come quelli sanitari, è invece permesso se ricorrono interessi pubblici di tutela di diritti fondamentali, per lo Stato o per l'Europa.
La tutela del diritto alla salute è tanto importante che i trattamenti effettuati per necessarie finalità di cura (art. 9, co. 2, lett. h e co. 3, GDPR) non necessitano del consenso del paziente, quando effettuati da, o sotto la responsabilità di, un operatore obbligato al segreto professionale.
Il consenso è invece richiesto per tutti quei trattamenti, solo in senso lato attinenti alla cura, che non sono direttamente causa della cura stessa: il consenso dev'essere raccolto per la refertazione online, per la tenuta del fascicolo sanitario elettronico, per l'utilizzo di app. mediche o per l'inoltro di messaggi promozionali e commerciali.
Al paziente dev'essere fornita un'informativa chiara, concisa e trasparente e si suggerisce di fornire le informazioni, previste dal GDPR, in modo progressivo: nei confronti della generalità dei pazienti potrebbero essere fornite solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione del servizio; mentre gli elementi informativi relativi a particolari attività di trattamento potrebbero essere resi, in un secondo momento, solo ai pazienti effettivamente interessati a ulteriori servizi.
Ultimi chiarimenti vengono dati dal Garante in ordine ai termini di conservazione dei dati: se non sono fissati da norme specifiche, è oggetto di responsabilizzazione del titolare fissare un periodo di conservazione congruo agli standard di legge. In ogni caso detti termini devo essere portati a conoscenza del paziente tramite l'informativa.

I medici di famiglia si confrontano con il regolamento europeo sulla privacy e scoprono che è più insidioso di come sembri: sulla carta non ci sarebbe bisogno del consenso del paziente al trattamento dei suoi dati ma è meglio raccoglierlo; non servirebbe il data protection officer al medico single, ma è meglio nominarlo, e così via. Gli adempimenti sono onerosi, a volte coinvolgono avvocati aggiornati oltre che esperti di protezione dati, e comunque spesso chi tratta dati sensibili all'altro capo del filo, come gli

ospedali (o il paziente a casa) non è altrettanto protetto. Il tema è emerso al Congresso Fimmg Lombardia, a Milano insieme alla notizia dell'imminente uscita di linee guida del Garante sul trattamento "sicuro" dei dati sanitari, dalla comunicazione al paziente al fascicolo sanitario, per continuare con gli obblighi di Dpo. In assenza di certezze però è bene prepararsi. Così, dopo aver aggiornato il registro trattamenti, il medico - titolare di questi ultimi- deve curare in questi mesi l'informativa, sapendo di dover trattare dati dei dipendenti e loro familiari, dei collaboratori (infermieri ad esempio), di soggetti terzi tra cui gli stessi responsabili del trattamento (commercialisti, enti di manutenzione rete informatica, società di videosorveglianza) e soprattutto dei suoi assistiti. Dovrà acquisire puntuale firma per presa visione delle informative come emerso dalle relazioni delle avvocatesse **Micaela Barbotti**, **Angela Berinati** e **Simona Custer** dello studio legale Albè e associati di Milano.

L'informativa al dipendente oltre a contenere dati di contatto del medico titolare e del Dpo eventuale, deve dire quali dati personali sono trattati, di chi (anche familiari se ci sono benefici fiscali, finalità del trattamento, motivi giuridici alla base di esso, se il trattamento avviene su carta o pc, a chi sono comunicati i dati (banche, assicurazioni, Inail in questo caso), i diritti dell'interessato, se i dati sono o meno a "rischio" di trasferimento a gestore o interlocutore estero. L'informativa per i pazienti deve dire quali sono i dati trattati - ci sono sensibili (sesso e salute) ma anche genetici e biometrici - per quali finalità, quali basi giuridiche ha il trattamento, a chi vengono riportati. Ai fini di tutela della salute, diagnosi e terapia, prevenzione, si affiancano attività di ricerca scientifica, partecipazione a trial, e pure, a volte, invio di newsletter sullo studio. Per il regolamento UE/GDPR le finalità di cura non richiederebbero obbligo di consenso ma la necessità di aggiornare l'informativa -per spiegare al paziente che i suoi dati vanno ad altri medici del gruppo, o a specialisti, ma anche a società di manutenzione Pc, Agenzia delle Entrate per il 730 precompilato in caso di prestazioni libera professione, nonché comunicargli i suoi diritti di accesso ai dati, alla loro cancellazione e portabilità etc - oggi fa pensare che la semplice affissione di un poster in sala d'attesa non dia la stessa sicurezza della consegna del modulo a mano in cambio di una firma per presa visione.

Altro tema spinoso il data protection officer, il GDPR esonera dalla nomina del Dpo chi tratti dati sensibili su larga scala, i Garanti Ue dicono che l'attività di medico single non è su larga scala ma siccome un medico

di famiglia può gestire dal 40 al 100% della popolazione di un paesino, il Garante italiano parrebbe orientato a livellare verso l'alto i meccanismi di tutela, e in ogni caso in mancanza di linee guida d'appoggio il consiglio è valutare caso per caso e vincere l'incertezza residua con la nomina di un Dpo. Che, si ricorda, è una "sicurezza", può stare allo studio come un portiere a una squadra di calcio; i data breach infatti, non sono infrequenti in sanità, solo lo scorso anno dall'entrata in vigore del GDPR ne sono stati notificati al Garante (com'è d'obbligo) 630, e ci sono state oltre 13.835 richieste di contatto all'Authority per chiarimenti sul tema della sicurezza dati. Per non parlare della videosorveglianza, altro capitolo scottante che in caso di presenza di dipendenti richiede informative ad hoc con consensi, cartellonistica aggiornata al 2018, valutazione d'impatto dei trattamenti, procedure (policies) per attestare il rispetto degli obblighi normativi. Dalla platea del congresso, tra le altre cose, viene la richiesta di capire quali norme ora regolino la corrispondenza via mail con i pazienti, sempre più fitta, e quali responsabilità ci siano se ad essere "fallati" siano i dispositivi di ricezione del paziente, o quali colpe abbia il medico ospedaliero che riceva una corrispondenza con dati sensibili su un account gestito e protetto dall'ospedale; domande che al momento non hanno risposte.