QUANDO PARLO CON IL MIO MEDICO CON QUANTI PARLO?

LA RISERVATEZZA IN SANITÀ E NEI SERVIZI TOSSICODIPENDENZE

DI
MARIAGRAZIA FASOLI

AGGIORNATO AD AGOSTO 2023

(prima versione: Fasoli M., marzo 2004; seconda versione: Fasoli M., Rossi Romano D., novembre 2010; terza versione Fasoli M., Rossi Romano D., gennaio 2016)

Premessa

Negli ultimi anni, In Italia e in Europa, la normativa sulla riservatezza è stata oggetto di continui aggiornamenti in tutti i settori, compreso quello sanitario. Una normativa "instabile" è generalmente un indicatore di tensioni e conflitti tra sistemi di valori tra loro non sempre compatibili. Per i medici e gli altri operatori sanitari la traduzione in pratica di tutto ciò può essere un aumento di "carte" più o meno informatizzate, burocrazia, contenziosi, stress lavorativo. Scopo di questa nota è rendere più semplice l'applicazione di diritti e doveri partendo dalla lontana esperienza del SER.T. di Montichiari (BS) dove dal 1985 al 2003 le regole ora divenute legge furono procedure del servizio, senza che ciò determinasse particolari problemi e, anzi, consentendo interessanti e altrimenti impossibili sviluppi anche dal punto di vista clinico e scientifico. Il *Decreto Legislativo (D.Lgs.) 30 giugno 2003 n.196* (come modificato dal D. Lgs 10 agosto 2018 n.101), "*Codice in Materia di Protezione dei Dati Personali"*, e il *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, 27 aprile 2016"*, abbreviato in GDPR, sono le norme di riferimento per la tutela della riservatezza nel nostro paese e nell'Unione Europea. Tuttavia siamo ancora lontani, a giudicare dal numero e dalla entità delle sanzioni irrogate dal Garante in particolare alle aziende sanitarie pubbliche e private (e anche dall'atteggiamento di molti operatori) dal raggiungere gli obbiettivi che il legislatore si è proposto: garantire in concreto, e non solo astrattamente, ad ogni persona la "titolarità primaria" dei dati che la riguardano cioè di sé stessa come soggetto sociale. Come dimostrano proprio i continui tentativi di aggirare queste norme con i più svariati pretesti, la gestione dei dati personali altrui è una forma di potere a cui non tutti vogliono rinunciare. Purtroppo questa resistenza si è verificata, in alcuni casi, anche da parte di amministrazioni regionali o locali o di lobbies burocratiche o professionali. In questi casi, l'operatore, gerarchicamente dipendente da queste amministrazioni, potrebbe trovarsi particolarmente in difficoltà. Riteniamo che l'adesione allo spirito della legge e l'attenzione alla lettera di ogni provvedimento possano essere un buon modo per superare ogni problema, anche perché in caso di dubbio è sempre possibile rivolgersi alla Autorità Garante per delucidazioni. In caso di violazioni di interesse pubblico, inoltre, il recente *D. Lgs. 24/2023 "Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali."* prevede esplicitamente la possibilità per dipendenti pubblici e privati di segnalare alla Autorità Nazionale Anticorruzione (ANAC) eventuali illeciti riguardanti tutela della vita privata, protezione dei dati personali e sicurezza delle reti e dei sistemi informativi e ciò in totale riservatezza e sicurezza. Vale la pena di farlo. Per chi si dedica alle professioni di aiuto, infatti, queste norme dovrebbero rappresentare l'evoluzione di un fatto di civiltà, da oltre 2000 anni implicito nel concetto di segreto professionale: il riconoscimento dell'individuo come "proprietario" della propria vita e della propria storia,

anche di fronte a diversi interessi della collettività o del potere politico, religioso o economico.
Sottolineiamo infine che il contenuto di questa nota rappresenta esclusivamente il punto di vista delle autrici che non hanno particolari competenze di tipo giuridico ma hanno svolto per anni funzioni di direzione e consulenza di servizi pubblici in area dipendenze.
Abbiamo voluto con ciò mettere a disposizione dei colleghi non tanto la nostra specifica competenza quanto la nostra concreta esperienza in un settore in cui, a volte, il povero operatore ha l'impressione di essere circondato da Azzeccagarbugli in contrasto l'uno con l'altro e, per restare in clima manzoniano, si sente come un vaso di coccio tra vasi di ferro.
Poiché si tratta, però, di materia di rilevanza (anche) penale, suggeriamo, in caso di dubbi, di consultare direttamente il sito del Garante contenente le norme citate o di interpellare l'ufficio legale del proprio ordine o collegio professionale.

Brescia, Agosto 2023

Riservatezza, deontologia professionale e diritti umani

Il concetto di "diritti umani" fa riferimento ad una concezione filosofico-politica secondo cui alcuni diritti fondamentali sono "naturalmente" connessi alla sola qualità di essere umano ed hanno quindi un'applicazione universale ed una forza superiore a qualsiasi altra norma. Sebbene molto antico, questo concetto ha trovato la sua prima esplicitazione in epoca moderna con la Dichiarazione Universale dei Diritti dell'Uomo e del Cittadino adottata nel 1789 dal governo rivoluzionario francese. Attualmente fanno riferimento a questo genere di diritti numerosi documenti internazionali, il più noto dei quali è la Dichiarazione Universale dei Diritti dell'Uomo siglata a Parigi il 10 dicembre 1948 come documento base delle neo-costituite Nazioni Unite. Il diritto alla riservatezza, in passato in vari modi riconosciuto da molte costituzioni democratiche, è attualmente contemplato come diritto fondamentale anche nell'art. 8 della Convenzione Europea dei Diritti dell'Uomo che recita: *"Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui."* Anche la Costituzione della Repubblica Italiana tutela espressamente la riservatezza come diritto fondamentale dell'uomo (indipendentemente, quindi, dalla cittadinanza italiana), vietando ogni forma di ispezione o perquisizione personale (articolo 13), proclamando l'inviolabilità del domicilio (articolo 14) e garantendo "*la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione*" (articolo15). Eccezioni sono previste solo *"per atto motivato dall'autorità giudiziaria e nei soli casi e modi previsti dalla legge"*. Da parte sua l'Unione Europea, prima con la direttiva del Parlamento Europeo e del Consiglio dell'Unione n. 95/46/CE del 24 ottobre 1995, e poi con il *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, 27 aprile 2016* obbligò gli stati membri ad assicurare "*la protezione delle libertà e dei diritti fondamentali delle persone fisiche, in particolare della loro vita privata, rispetto al trattamento dei dati personali*". In quanto diritti umani, queste garanzie si applicano a chiunque, per qualunque tipo di dati personali e rappresentano il risultato della secolare evoluzione degli Stati Europei verso la democrazia. Nella tradizione occidentale e mediterranea, classica, cristiana, ebraica ed islamica però, da quasi tremila anni, si riconosce anche un altro tipo di segreto, imposto da alcuni "ordini" professionali o sacerdotali ai propri membri, spesso attraverso un giuramento solenne. Questo tipo di riservatezza può essere riconosciuta anche dagli Stati, ma fondamentalmente deriva dalla deontologia professionale che potrebbe essere definita "la moralità delle professioni". Chi oggi si rivolge ad un medico o ad una struttura sanitaria gode quindi di una doppia protezione: come persona ha diritto alla riservatezza e alla "proprietà" dei propri dati personali e come paziente ha diritto al rispetto del segreto professionale, peraltro riconosciuto dalla legislazione italiana.

Segreto professionale

Il segreto professionale è il diritto alla riservatezza che viene riconosciuto a chi si rivolge ad un medico, ad un avvocato o ad un sacerdote e che oggi si è esteso anche ad altre professioni come quella dello psicologo e dell'infermiere professionale.

La prevalenza, anche sull'interesse collettivo (si pensi all'autore di un delitto che ricorre ad un sacerdote o ad un avvocato), del diritto individuale a difendere, in certe circostanze, la propria libertà e la propria salute fisica, psichica, sociale e spirituale è stata storicamente imposta dagli stessi membri di quelle che oggi chiamiamo "professioni d'aiuto" ed è (o dovrebbe essere) considerata una condizione fondante del rapporto professionista–cliente. Per questo motivo, anche quando la legge, come avviene nel nostro paese, riconosce o addirittura impone il rispetto del segreto professionale, sono ancora gli Ordini e i Collegi professionali a stabilire, attraverso l'emanazione di codici deontologici, le regole di comportamento a cui tutti gli iscritti devono attenersi.
Il Codice di Deontologia Medica 2014 (d'ora in poi CDM), per esempio, dispone (artt. 10, 11 e 12), che *"il medico deve mantenere il segreto su tutto ciò di cui è a conoscenza in ragione della propria attività professionale".* Inoltre *"il medico non deve rendere all'Autorità competente in materia di giustizia e di sicurezza testimonianze su fatti e circostanze inerenti il segreto professionale".* Norme analoghe, o anche più rigide, sono dettate dai Codici Deontologici degli psicologi, degli infermieri, degli assistenti sociali e degli educatori.
Tutto ciò significa che, senza il consenso dell'interessato (se maggiorenne) o senza il consenso dei genitori o del tutore o curatore (se minorenne o incapace) nessuna informazione sui nostri pazienti dovrebbe essere fornita né ai famigliari né ad altri (ivi compresa la magistratura, come si vedrà più oltre) con alcune eccezioni espressamente previste sia dalla legge sia dagli stessi Codici Deontologici.
Il professionista che non si attenesse a queste regole potrebbe incorrere in sanzioni disciplinari, quali ad esempio, la sospensione dall'Ordine per un certo periodo e la conseguente impossibilità di esercitare. Il professionista dovrebbe anche vigilare affinché il segreto sia mantenuto dai suoi collaboratori. A questo proposito, particolare attenzione deve essere posta nei rapporti con persone che non esercitano professioni sanitarie (per esempio volontari od operatori sociali di organizzazioni non sanitarie) e che perciò non hanno né il diritto né il dovere di mantenere questo particolare tipo di segreto.
Come si è detto il segreto professionale è riconosciuto, in Italia, anche dalle leggi dello Stato. L'articolo 622 del Codice Penale (d'ora in poi CP), infatti, punisce con la reclusione la violazione del segreto professionale, ma solo nel caso che la rivelazione produca un danno. L'articolo 200 del Codice di Procedura Penale (d'ora in poi CPP) dispone, invece, che sacerdoti di qualunque religione ammessa dallo Stato, avvocati, medici, farmacisti, levatrici e ogni altro esercente una professione sanitaria "*non possono a pena di nullità essere obbligati a deporre su ciò che a loro fu confidato o pervenuto a loro conoscenza per ragione del proprio ministero o ufficio o della propria professione".* Inoltre, nel nostro paese, per esercitare una professione, anche come lavoratori dipendenti, è obbligatorio essere iscritti all'Ordine e, quindi, rispettarne le regole.
Segnaliamo che, a differenza del precedente, il CDM in vigore non prevede tassativamente le eccezioni alla regola generale del segreto ma rimanda la liceità della rivelazione ad *"una giusta causa prevista dall'ordinamento o dall'adempimento di un obbligo di legge".* Questa nuova formulazione, che, di fatto, rimanda allo Stato la decisione di rispettare o no il segreto, è stata fortemente criticata, in particolare da alcuni Ordini Provinciali. Si è infatti osservato che, con questa logica, si giustificherebbero, a rigore, persino i medici che in vigenza di leggi razziali od omofobe (peraltro tuttora in vigore in alcuni paesi) avessero denunciato alle autorità le persone non ariane od omosessuali. Più rigorosa, ad esempio, appare la tutela del segreto professionale nel Codice Deontologico degli Psicologi Italiani che agli artt. 12,13,14 e 15 limita la deroga ai casi di obbligo di referto o di denuncia (quindi quando sussiste un'ipotesi di reato che non coinvolga il cliente) e, anche in questi casi limitando "*allo stretto necessario il riferimento a quanto appreso in ragione del proprio rapporto professionale".*

Come illustrato più oltre, infine, per chiunque operi nei Servizi per le Dipendenze, il legislatore ha previsto all'art. 120 del DPR 309 del 1990 un particolare rinforzo del segreto professionale che equipara questi operatori all' avvocato difensore.

Segreto professionale e segreto d'ufficio

Tutti i pubblici impiegati sono obbligati a non divulgare "*notizie d'ufficio le quali debbano rimanere segrete"* pena la reclusione da sei mesi a tre anni (art. 326 CP). In base a questo articolo, tuttavia, è perfettamente possibile (e, a volte, è doveroso) trasferire qualsiasi notizia di interesse per altro ufficio ad altri impiegati della pubblica amministrazione, a loro volta obbligati al segreto d'ufficio. In questa trasmissione, è irrilevante la volontà dell'utente o il suo eventuale interesse a non far sapere qualcosa a qualche particolare struttura pubblica ma, al contrario, l'interesse generale rimane prevalente su quello individuale. Citiamo un esempio: i dati sulla proprietà di immobili di una persona non verranno forniti dal Comune ai curiosi, ma certo, in caso di necessità, verranno passati ad un altro ente pubblico che ne faccia richiesta (per esempio alla Agenzia delle Entrate per controlli fiscali), anche se ciò potrà danneggiare l'interessato. Il riconoscimento del segreto professionale permette, invece, a chi esercita le professioni sopra citate, anche come dipendente pubblico, di far prevalere l'interesse dell'utente anche quando è in conflitto con quello dello Stato, fino al punto di potersi addirittura rifiutare di testimoniare in tribunale. Perciò il medico, anche pubblico dipendente, al corrente del fatto che un suo paziente ha un'officina totalmente in nero, se, ad esempio, richiesto di fornire informazioni alla guardia di finanza, opporrà il segreto professionale. L'impiegato dell'ARPA, che pure si occupa di salute, chiaramente no.

Reati e segreto professionale nei Servizi per le Dipendenze

Il segreto professionale non comporta che i servizi sanitari diventino luoghi dove sia consentito commettere reati. L'articolo 331 del CPP impone infatti a tutti i pubblici ufficiali o incaricati di pubblico servizio l'obbligo di denunciare per iscritto "*senza ritardo*" i reati perseguibili d'ufficio (cioè tutti quelli per cui il codice non prevede che si proceda solo su denuncia di parte) di cui abbiano notizia nell'esercizio o a causa delle proprie funzioni (commi 1 e 2), anche quando non ne sia individuabile l'autore. Se più addetti hanno avuto notizia o hanno constatato i fatti, sono tutti ugualmente obbligati alla denuncia anche se possono anche redigere e sottoscrivere un unico atto (comma 3). L'omessa denuncia è, infatti, un reato (punibile con una multa) previsto dagli artt. 361 e 362 CP e pertanto ognuno ne risponde personalmente. La denuncia deve essere inoltrata o al pubblico ministero o a un ufficiale di polizia giudiziaria (art. 331 CPP, comma 2) e deve contenere la esposizione degli elementi essenziali del fatto, il giorno dell'acquisizione della notizia, le fonti di prova già note, quanto serva a identificare la persona a cui è attribuito il fatto, la persona offesa e coloro che siano grado di riferire su circostanze rilevanti per la ricostruzione dei fatti (art. 332 CPP). Ricordiamo che riveste il ruolo di addetto a pubblico servizio chiunque stia svolgendo attività che realizzano la volontà della pubblica amministrazione. Quindi, ad esempio un professionista operante al SERT agisce come addetto a pubblico servizio indipendentemente dal tipo di contratto mentre così non è quando svolge la libera professione. Per quanto riguarda il personale sanitario, trova applicazione anche l'art. 365 del CP concernente l'obbligo di referto. Tale articolo dispone che sia punito con una multa "*chiunque, avendo nell'esercizio di una professione sanitaria prestato la propria assistenza od opera in casi che possono presentare i caratteri di un delitto pel quale si debba procedere d'ufficio, omette o ritarda*" di riferirne all'autorita' giudiziaria ma aggiunge che "*questa disposizione non si applica quando il referto*

esporrebbe la persona assistita a procedimento penale". Il referto deve essere inoltrato entro 48 ore (art. 334 CPP) o, in caso di pericolo, immediatamente al pubblico ministero o a qualsiasi ufficiale di polizia giudiziaria. Il termine "chiunque" include, appunto, chiunque eserciti una professione sanitaria e si riferisce quindi anche ai sanitari dipendenti pubblici o addetti a pubblico servizio. Costoro quindi non dovrebbero denunciare casi che potrebbero esporre la persona assistita a procedimento penale. Che questa sia la volontà del legislatore è dimostrato anche dall'applicabilità ai sanitari pubblici dipendenti dell'art. 200 CPP (esenzione dall'obbligo di testimoniare in giudizio per fatti coperti dal segreto professionale) ed è ribadito dall' art. 256 dello stesso CPP concernente il "dovere di esibizione e segreti" che dispone quanto segue: *"Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di stato ovvero di segreto inerente al loro ufficio o professione. Quando la dichiarazione concerne un segreto d'ufficio* (da intendere ufficio di culto, cfr art 200 CP ndr) *o professionale, l'autorità giudiziaria, se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti, i documenti o le cose indicati nel comma 1, provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro."* Per quanto riguarda il personale dei servizi tossicodipendenze (ma non per quello di altre strutture sanitarie, psichiatria compresa), inoltre, questa interpretazione è rinforzata anche dall'art. 120 del citato DPR 309/1990 che (comma 7) dispone che gli operatori del servizio pubblico per le tossicodipendenze e delle strutture private autorizzate "*non possono essere obbligati a deporre su quanto hanno conosciuto per ragione della propria professione, ne' davanti all'autorita' giudiziaria ne' davanti ad altra autorita'. Agli stessi si applicano le disposizioni dell'articolo 200 del codice di procedura penale e si estendono le garanzie previste per il difensore dalle disposizioni dell'articolo 103 del codice di procedura penale in quanto applicabili.*" L'art. 103 del CPP dispone quanto segue: *"Le ispezioni e le perquisizioni negli uffici dei difensori sono consentite solo: a) quando essi o altre persone che svolgono stabilmente attività nello stesso ufficio sono imputati (60, 61), limitatamente ai fini dell'accertamento del reato loro attribuito; b) per rilevare tracce o altri effetti materiali del reato o per ricercare cose o persone specificamente predeterminate. Nell`accingersi a eseguire una ispezione, una perquisizione o un sequestro nell`ufficio di un difensore, l`autorità giudiziaria a pena di nullità avvisa il consiglio dell`ordine forense del luogo perchè il presidente o un consigliere da questo delegato possa assistere alle operazioni. Allo stesso, se interviene e ne fa richiesta, è consegnata copia del provvedimento. Alle ispezioni, alle perquisizioni e ai sequestri negli uffici dei difensori procede personalmente il giudice ovvero, nel corso delle indagini preliminari, il pubblico ministero in forza di motivato decreto di autorizzazione del giudice. (…) Sono vietati il sequestro e ogni forma di controllo della corrispondenza tra l`imputato e il proprio difensore in quanto riconoscibile dalle prescritte indicazioni salvo che l`autorità giudiziaria abbia fondato motivo di ritenere che si tratti di corpo del reato. Salvo quanto previsto dal comma 3 e dall`art. 271, i risultati delle ispezioni perquisizioni, sequestri, intercettazioni di conversazioni o comunicazioni, eseguiti in violazione delle disposizioni precedenti, non possono essere utilizzati."* Ciò non ostante, alcune scuole di medicina legale hanno ritenuto che i pubblici dipendenti e gli addetti a pubblico servizio, compresi coloro che operano nei servizi per le dipendenze, abbiano sempre l'obbligo di denuncia e che l'obbligo di referto si riferisca solo a liberi professionisti. La questione venne sollevata per sostenere che la legge 94/2009, introducendo il reato di immigrazione clandestina, avrebbe costretto i medici dipendenti pubblici a denunciare i pazienti stranieri

iregolari. Sia la FNOMCeO sia la circolare Ministero Interni 780/A7 n. 12 del 27-11-2009 esclusero però questa ipotesi citando, tra l'altro, proprio l'art. 365 CP. Pertanto l'obbligo di denuncia non sussiste per i reati attribuibili al paziente di cui si sia venuti a conoscenza nel corso o causa del rapporto terapeutico.

Giusta causa di rivelazione del segreto professionale

Come si è detto, i reati che una persona commette all'interno o ai danni di una struttura sanitaria, comportandosi così, letteralmente, da "delinquente" e non da paziente, (esempio: furti ai danni di altri degenti, aggressioni, spaccio) devono invece essere immediatamente denunciati, sia per motivi assicurativi sia per non essere poi accusati dalle vittime di corresponsabilità in ulteriori danni. In questi casi dovrà, come sempre, essere indicato nella denuncia tutto ciò che sia pertinente alla valutazione del fatto, anche se si trattasse di informazioni (come ad esempio l'indirizzo o le abituali frequentazioni dell'interessato) apprese nel corso del rapporto di cura. Non c'è infine alcun dubbio sull'obbligo di immediata denuncia (e di richiesta di intervento delle forze dell'ordine, se necessario) nel caso ci siano elementi che indichino la concreta possibilità che un paziente stia per commettere un reato che metta in pericolo la vita o la salute di terzi. In questo caso, infatti, prevale il dovere di salvaguardare l'incolumità di terze persone peraltro considerato preminente anche nell'art. 54 del CP che recita, riferendosi ad eventuali reati (quale potrebbe essere la rivelazione di segreto professionale): *"Non è punibile chi ha commesso il fatto per esservi stato costretto dalla necessità di salvare sè od altri dal pericolo attuale di un danno grave alla persona, pericolo da lui non volontariamente causato, nè altrimenti evitabile, sempre che il fatto sia proporzionato al pericolo."* Casi di questo genere sono i maltrattamenti di minori (purchè dedotti da fatti concreti e precisi) e anche le richieste di informazioni da parte delle forze dell'ordine in base alla legge 69/2019 "*Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere"*, cosiddetta del "codice rosso", il cui scopo è di consentire interventi immediati per prevenire gravi fatti di violenza.

Segreto professionale e diritto all'anonimato nei Servizi per le Tossicodipendenze

Il già citato DPR 309/1990, che regola il funzionamento dei Servizi Tossicodipendenze pubblici e privati accreditati (Servizi Multidisciplinari Integrati, SMI), prevede, all'articolo 120, che le persone che vi si rivolgono possano (comma 3) "*a loro richiesta beneficiare dell'anonimato nei rapporti con i servizi i presidi e le strutture delle Unità Sanitarie Locali nonché con i medici, gli assistenti sociali e tutto il personale addetto o dipendente"* e che (comma 6) "*coloro che hanno chiesto l'anonimato hanno diritto a che la loro scheda sanitaria non contenga le generalità né altri dati che valgano alla loro identificazione".* Chiunque si rivolga ad un Ser.T./SMI, pertanto ha il diritto di essere curato/a senza dare il proprio nome. Il comma 9 del medesimo articolo 120 dispone che *"la scheda sanitaria* (che le regioni avrebbero dovuto elaborare in base al comma 8, n.d.r.) *preveda un modello di codifica atto a tutelare il diritto all'anonimato del paziente e ad evitare duplicazioni di carteggio*". Poiché il sistema di codifica non è stato per ora definito dalle regioni, al paziente che chiede l'anonimato potrà essere attribuita una sigla da parte del servizio. Benchè ciò si presti ad ipotesi di illegittimità per violazione del principio di uguaglianza tra i cittadini, chi decide di usufruire dell'anonimato, però, non può, di fatto, avere accesso a prestazioni che altre normative consentono solo previa identificazione. In particolare: non può ottenere certificati per l'esenzione dal ticket; non può usufruire di finanziamenti pubblici per il pagamento di rette in comunità terapeutiche accreditate; non può ottenere

certificati di tossicodipendenza; qualora fosse in trattamento con metadone o altri farmaci oppioidi, non può essere trasferito ad altri servizi in cui non sia direttamente conosciuto, sebbene con una sigla; non può ottenere copia della cartella clinica. Non sussistono invece problemi per i trattamenti sostitutivi con oppioidi effettuati presso il servizio dato che l'articolo 64 del DPR 309/1990 fa sì obbligo di riportare le generalità dei pazienti sul registro degli stupefacenti, ma sembra escludere esplicitamente chi rientra nella fattispecie dell'articolo 120, pur rinviando, per evidente svista del legislatore, al comma 4 (abrogato per referendum popolare e non pertinente) anziché al comma 5. Anche per chi non chiede l'anonimato lo stesso articolo 120 prevede uno speciale rafforzamento del segreto professionale disponendo (comma 7), come già accennato, che "*i dipendenti del servizio pubblico per le tossicodipendenze"* (compresi quindi coloro che non esercitano professioni sanitarie, come gli amministrativi), "*non possono essere obbligati a deporre né davanti all'autorità giudiziaria né davanti ad altra autorità*". Tale norma viene inoltre estesa anche a "*coloro che operano presso enti, centri, associazioni o gruppi convenzionati con i servizi pubblici per il trattamento delle tossicodipendenze*". Allo stesso personale inoltre vengono estese le garanzie che l'articolo 103 del CPP riserva all'avvocato difensore. In particolare, come si è visto, tale articolo vieta anche alla magistratura le perquisizioni, il sequestro di documenti, le intercettazioni telefoniche, il sequestro o ogni forma di controllo della corrispondenza presso le sedi dei servizi se non per accertare reati commessi dal personale o per cercare cose o persone specificamente determinate. Ciò deve essere fatto, però, personalmente dal giudice o dal pubblico ministero e solo alla presenza del presidente o di un consigliere dell'Ordine Professionale.
Ricordiamo infine che Il DPR 309/1990 è una legge nazionale speciale in quanto specificamente diretta a regolare tutto quanto riguarda gli stupefacenti. In caso di conflitto tra norme vale il principio che "lex specialis derogat generalis" e "lex superior derogat inferiori". Ciò significa che, se la stessa materia è disciplinata da più norme di cui una generale e l'altra speciale, quest'ultima prevale sulla prima a prescindere da quale sia la più recente. Inoltre una materia è regolata da una legge statale questa prevale su eventuali leggi regionali che la contraddicano.

Rapporti fra colleghi

Da tutto ciò si deduce che chi opera in un Servizio per le Tossicodipendenze non deve, senza esplicita autorizzazione dell'interessato, trasferire informazioni coperte da segreto professionale ad operatori od altri soggetti che non godano delle stesse garanzie (come per esempio il personale non sanitario di altri servizi o il personale sociale dei comuni o "volontari" di cooperative) mentre tale trasferimento è possibile verso i professionisti che collaborano alla gestione del caso o nei confronti dell'avvocato di fiducia del paziente, ovviamente solo per quanto di suo specifico interesse. Infatti tale professionista assume il ruolo di rappresentante del suo assistito e gode di tutte le garanzie riconosciute al personale dei Ser.T/SMI comprese quelle contenute nell'articolo 103 CPP. I rapporti con altri professionisti coinvolti nella cura del paziente sono invece regolati, per quanto riguarda i medici, dagli articoli 58, 59, 60, 61, 66 del CDM, ed analoghe prescrizioni sono contenute nei codici deontologici degli psicologi, degli assistenti sociali, degli infermieri e degli educatori. Tali disposizioni, in sintesi, stabiliscono che:

- il terapeuta è tenuto a fornire ai colleghi che collaborano direttamente alla cura le informazioni e la documentazione necessaria a diagnosi e terapia;
- ciò deve avvenire previo consenso dell'interessato o del suo rappresentante legale;
- qualunque altro uso delle informazioni (per esempio a scopo didattico o di ricerca) deve essere esplicitamente e liberamente autorizzato dal paziente, previa adeguata informazione.

Segreto epistolare

Le particolari garanzie previste dalla legge per chi si rivolge ai Ser.T./SMI valgono anche per il segreto epistolare, tutelato specificamente dal comma 7 dello stesso articolo 103 CPP oltre che, genericamente, dall'articolo 15 della Costituzione e dall'articolo 616 del CP. Pertanto la posta indirizzata a personalmente a professionisti operanti nei Servizi Tossicodipendenze (e non genericamente alla struttura o alla carica), in quanto potenzialmente contenente informazioni coperte dal segreto professionale, non può essere aperta se non da personale del servizio, dato che al restante personale ASL non si estende l'articolo 103 CPP. Come da disposizione del citato art. 616 CP "*per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza"*
Anche a queste ultime modalità di comunicazione, quindi, se indirizzate dal mittente espressamente a un professionista del Servizio Tossicodipendenze in specifica casella postale, devono ritenersi applicabili le norme sopra citate.

Il Regolamento (UE) 2016/679 (GDPR) e il Decreto Legislativo 196/2003 "Codice in materia di protezione dei dati personali"

I diritti dei cittadini rispetto all'uso dei dati personali, compresi quelli forniti ai Servizi Sanitari, sono garantiti, oltre che dalle norme deontologiche e dalle nostre leggi penali, anche dal Regolamento (UE) 2016/679 (General Data Protection Regulation, d'ora in poi GDPR, direttamente in vigore negli stati membri dell'Unione) e dal Decreto Legislativo 196/2003 "Codice in Materia di Protezione dei Dati Personali". Purtroppo il legislatore, dopo il 2016, non è stato in grado di produrre un nuovo Codice adeguato alle disposizioni del Regolamento ed ha preferito emendare quello precedente creando notevoli difficoltà alla consultazione da parte dei cittadini. In ogni caso, il principio fondamentale a cui si ispira tutta la normativa comunitaria e nazionale è che i dati personali sono "proprietà" di chi li fornisce e quindi, salvo eccezioni previste tassativamente dalla legge, possono essere utilizzati, trattati e conservati solo per gli scopi, il tempo e con i modi autorizzati dall'interessato. La protezione della riservatezza si configura quindi, come si è detto, come un vero e proprio diritto umano che prescinde da qualunque requisito di appartenenza, condizione o cittadinanza. L'art. 1 del GDPR sancisce infatti la protezione dei "*diritti e libertà fondamentali delle persone fisiche in particolare il diritto alla protezione dei dati personali"*.
L'articolo 5 del Regolamento definisce quindi i principi per il trattamento dei dati personali. I dati devono essere (comma 1):

- "trattati in modo lecito corretto e trasparente nei confronti dell'interessato" ("liceità correttezza e trasparenza");
- "raccolti per finalità determinate, esplicite e legittime" ("limitazione delle finalità");
- "adeguati pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" ("minimizzazione dei dati");
- "esatti e se necessario aggiornati"("esattezza"),
- "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati" ("limitazione della conservazione")
- "trattati in maniera da garantire una adeguata sicurezza" ("integrità e riservatezza")

Il titolare del trattamento è responsabile del rispetto della norma e deve essere in grado di provarlo ("responsabilizzazione", comma 2).

Definizioni (articolo 4 GDPR e art. 2 ter del Codice)

Il Regolamento chiarisce all'articolo 4 il preciso significato dei termini usati. Riportiamo di seguito le principali definizioni.

- "dato personale": qualsiasi informazione riguardante persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali
- «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
- «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- «dati 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;

- «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;
- «dati 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;

Inoltre l'art. 2 ter, comma 4 del Codice così definisce i seguenti concetti:

a) "comunicazione", il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato (…) in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Richiamiamo l'attenzione sulle diverse posizioni del titolare e del responsabile del trattamento. Il titolare risponde della legittimità e correttezza delle finalità e delle modalità del trattamento ma non tratta i dati. Il responsabile, invece, tratta direttamente i dati seguendo le procedure e per le finalità definite dal titolare. In pratica, in ambito sanitario, l'ente risponde come titolare ma solo i professionisti possono trattare i dati a meno che non siano anonimizzati o che una disposizione di legge lo consenta espressamente, salvo quanto eventualmente disposto dalle leggi speciali come il DPR 309/1990.

L'art. 2 quatterdecies del Codice individua inoltre la figura dei *"soggetti designati"* disponendo che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilita' e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorita'".* In genere nelle aziende sanitarie titolare del trattamento è il rappresentante legale cioè il direttore generale mentre responsabili sono i capiservizio (di regola direttori di struttura complessa). Costoro sono tenuti ad attribuire ai loro collaboratori (i designati) i compiti strettamente necessari al trattamento dei dati indispensabili per lo svolgimento delle proprie funzioni. L'accesso generalizzato di tutto il personale ad ogni genere di dati di tutti i pazienti non è quindi mai consentito a meno di dimostrarne la assoluta necessità per i compiti istituzionali.

Il Responsabile della Protezione dei Dati (art 37 GDPR)

L'art. 37 del GDPR obbliga il titolare del trattamento effettuato da autorità o organismi pubblici a nominare un responsabile della protezione dei dati. Costui deve essere designato (comma 5) "*in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati"* e può essere sia un dipendente dell'ente sia un consulente esterno. In ogni caso (art. 38) deve essere fornito delle risorse necessarie a svolgere i suoi compiti, non deve ricevere istruzioni dal titolare, non può essere rimosso o penalizzato per quanto fatto nell'esercizio delle sue funzioni e non deve trovarsi in conflitto di interessi. Gli interessati possono rivolgersi direttamente a lui per tutte le questioni relative ai propri diritti.

I compiti del Responsabile della Protezione dei Dati, definiti dall'art. 39, sono i seguenti: a) informare e fornire consulenza a titolare, responsabile e dipendenti; b) sorvegliare l'osservanza del Regolamento, c) fornire pareri sulla valutazione d'impatto delle procedure sulla sicurezza dei dati d) cooperare con l'autorità Garante e) fungere da collegamento con il Garante rispetto a qualunque questione rilevante.

Il Garante per la Protezione dei Dati Personali

Gli articoli 51-67 del GDPR impongono agli stati membri di istituire una autorità di controllo indipendente per la applicazione del Regolamento e ne definiscono modalità di nomina, compiti e poteri elencati agli articoli 57 e 58. Oltre a compiti di sorveglianza il Garante (istituito in Italia già con la legge 31 dicembre 1996 n. 675) ha anche poteri normativi e sanzionatori indipendenti dal governo e dalla autorità giudiziaria per la cui illustrazione si rimanda al sito www.garanteprivacy.it. Ogni cittadino può consultare su questo sito norme, provvedimenti e indicazioni relativi alla riservatezza.

Le categorie particolari di dati personali (articolo 9 GDPR)

L' articolo 9 del GDPR identifica un particolari categorie di dati personali (già citati nella precedente normativa italiana come "dati sensibili") il cui trattamento è di regola vietato (comma 1). Tale articolo stabilisce che "*è vietato trattare dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco la persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona"*. Le eccezioni a tale divieto sono tassativamente indicate al comma due. Per quanto di competenza dei servizi sanitari, in particolare il trattamento è consentito nei casi in cui: a) l'interessato ha prestato consenso esplicito per una o più finalità specifiche c) è necessario per un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nella incapacità fisica o giuridica di prestare il proprio consenso; e) riguarda dati resi manifestatamente pubblici dall'interessato; oppure f) per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni; h) per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali; i) per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici purchè proporzionato alla finalità perseguita e nel rispetto di diritti fondamentali e interessi dell'interessato.
Tuttavia, anche in questi casi, (comma 3) il Regolamento stabilisce che i dati indicati nel paragrafo 2, lettera h riguardanti, tra l'altro, la diagnosi, assistenza o terapia sanitaria o sociale ovvero la gestione dei sistemi e servizi sanitari o sociali possono essere trattati solo "*da o sotto la responsabilità di un professionista soggetto al segreto professionale (…) o da altra persona anch'essa soggetta all'obbligo di segretezza".*
I dati personali comunicati e trattati dal Servizio Tossicodipendenze rientrano di per sé in questa categoria. Il solo fatto di essere in carico ad un Ser.T./SMI o ad una comunità per tossicodipendenti, infatti, è informazione atta a rivelare che si è o si è stati tossicodipendenti, anche se si tratta di semplici dati anagrafici. Peraltro, come si vedrà più oltre, una serie di altri provvedimenti normativi, richiamano le particolari ulteriori garanzie richieste per i "*dati soggetti a maggior tutela",* tra i quali quelli riguardanti l'uso di droghe o alcol, perché oggetto di prescrizioni di leggi speciali (che, come si è detto prevalgono sulle leggi ordinarie precedenti e successive, compreso il GDPR), tra cui il DPR 309/1990. Diverso è il caso di altri servizi amministrativi delle Aziende Sanitarie: la semplice iscrizione negli elenchi della medicina di base o in quello dei soggetti da sottoporre a

vaccinazione obbligatoria o a visita fiscale non rivela di per sé alcuna informazione sulla salute della persona.
A questo proposito l'art. 2 sexies, comma 1 bis del Codice dispone che, in ogni caso, il trattamento di dati sanitari per fini legittimi, tassativamente autorizzati da una legge, (ivi compresi quelli contenuti nel Fascicolo Sanitario Elettronico) debbano essere trattati nel rispetto delle finalita' istituzionali di ciascuno "*privi di elementi identificativi diretti".*
I dati personali trattati in violazione di queste norme non possono essere utilizzati (art. 2 decies del Codice).

I diritti dell'interessato

Il Regolamento definisce i diritti dell'interessato agli articoli 12-22. Riportiamo sinteticamente il contenuto degli articoli 12-18 in quanto pertinenti anche ai trattamenti effettuati dai servizi sanitari.

Art. 12 - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

Obbliga il titolare a fornire all'interessato tutte le informazioni relative al trattamento dei suoi dati "*in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro".* Le informazioni sono fornite per iscritto o con altri mezzi, purché sia accertata l'identità dell'interessato. Ciò deve avvenire senza ritardo e, in ogni caso entro un mese dalla richiesta, prorogabile di due mesi in casi particolarmente complessi e dopo aver spiegato dettagliatamente all'interessato i motivi del ritardo. Qualora il titolare ritenga di non poter ottemperare alla richiesta deve comunicarne i motivi ed informare l'interessato delle modalità con cui fare ricorso.

Art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

L'interessato deve ricevere informazioni preliminari su: identità del titolare e dati di contatto del responsabile del trattamento e del Responsabile della Protezione dei Dati, finalità e base giuridica del trattamento, destinatari o categorie di destinatari che avranno accesso ai dati, periodo di conservazione dei dati, diritto dell'interessato di chiedere l'accesso ai dati, rettifica, cancellazione, limitazione o opposizione al trattamento, diritto di reclamo al Garante, obbligatorietà o meno del conferimento dei dati per ottenere la prestazione.

Art. 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

In caso i dati non siano stati raccolti presso l'interessato è necessario comunicargli anche le informazioni disponibili sulla loro origine. Inoltre il titolare deve fornire una copia dei dati oggetto di trattamento ma senza ledere i diritti altrui.

Art. 15 – Diritto di accesso dell'interessato

L'interessato ha il diritto di ottenere dal titolare la conferma che sia o meno in corso un trattamento dei suoi dati personali e in tal caso, di ottenere l'accesso alle seguenti informazioni: finalità, tipo di dati, persone o categorie di persone a cui possono essere comunicati, periodo di conservazione, diritto di reclamo, origine dei dati, eventuale esistenza di un processo decisionale informatizzato. Inoltre il titolare deve fornire all'interessato una copia gratuita dei dati.

Art. 16, 17, 18 – Diritto di rettifica, diritto alla cancellazione (“diritto all’oblio”), diritto alla limitazione al trattamento

L'interessato ha diritto di ottenere senza ritardo la rettifica dei dati inesatti e l'integrazione dei dati incompleti, anche fornendo una dichiarazione integrativa. Ha diritto ad ottenere la cancellazione quando i dati non sono più necessari per le finalità per cui sono stati conferiti, quando ha revocato il consenso o ha inoltrato opposizione e non sussistono altre basi giuridiche per il trattamento e quando i dati sono stati trattati illecitamente. Ha diritto a limitarne il trattamento quando ne contesta l’esattezza, quando il trattamento è illecito ma non ne chiede la cancellazione ma la limitazione, quando sono necessari per l’esercizio di diritti oppure si è opposto al trattamento e si è in attesa di verifica dell’eventuale prevalenza dei motivi del titolare.

L’informativa all’interessato in sanità e nei servizi per le dipendenze

In ambito sanitario, le informazioni sopra descritte possono essere fornite anche attraverso avvisi esposti nelle sale d’attesa e sui siti internet degli enti. Devono comunque rispettare le indicazioni di chiarezza, completezza e trasparenza previste dall’art.12 del GDPR, in particolare per le modalità dei trattamenti informatizzati. Devono inoltre contenere le indicazioni necessarie per ottenere ulteriori informazioni sui propri dati e su come accedervi facilmente. Non è quindi accettabile predisporre l’informativa come una generica “liberatoria” non solo perché, in questo modo si violerebbe lo spirito e la lettera della legge ma anche perché, paradossalmente, in caso di contestazioni, si fornirebbe la prova di non aver adeguatamente informato il cittadino. Le modalità di informazione sono precisate negli articoli 78 e 79 del Codice.
L’art. 78 riguarda le prestazioni di medici e pediatri di base e comporta che l’informativa riguardi anche i sostituti, gli associati, gli specialisti su richiesta del medico, i farmacisti per i farmaci prescritti. Inoltre questa informativa deve evidenziare “*analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonchè per la dignità dell'interessato, in particolare, tra l’altro, in caso di trattamenti effettuati: a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente; b)nell'ambito della teleassistenza o telemedicina; c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica; c-bis) ai fini dell'implementazione del fascicolo sanitario elettronico”.* L’art. 79 “*Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie*” estende alle aziende sanitarie la stessa possibilità di utilizzare un’unica informativa per una “*pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate.”* La avvenuta informazione deve essere annotata “*con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità’”.* L’informativa deve essere integrata (non sostituita) da cartelli e avvisi agevolmente visibili al pubblico e diffusi anche in pubblicazioni istituzionali o su siti internet (art. 80 del Codice). In sostanza ciò significa che quando un cittadino si rivolge ad un medico o ad un organismo sanitario per una prestazione che comporta necessariamente la collaborazione, anche indiretta, di altri (per esempio: farmacista, impiegato ASL, specialista consulente, supplenti di tutti costoro) l’informativa può essere rilasciata una sola volta da colui o coloro a cui l’interessato ha richiesto la prima prestazione.
Ulteriori precisazioni rispetto all’informativa sono contenute nel provvedimento del Garante n. 55 del 7 marzo 2019 *“Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario”.* Nel documento il Garante precisa che “*le infor-*

mazioni da rendere all'interessato vanno rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con linguaggio semplice e chiaro" e che *"spetta al titolare scegliere le modalità più appropriate al caso di specie, tenendo conto di tutte le circostanze del trattamento e del contesto in cui viene effettuato".* Le informazioni, inoltre, per facilitare la effettiva consapevolezza degli interessati, dovrebbero essere fornite in modo progressivo. In altri termini alla generalità dei pazienti *"potrebbero essere fornite solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività"* mentre *"gli elementi informativi relativi a particolari attività di trattamento (es. fornitura di presidi sanitari, modalità di consegna dei referti medici on-line, finalità di ricerca) potrebbero essere resi, infatti, in un secondo momento, solo ai pazienti effettivamente interessati da tali servizi e ulteriori trattamenti."*
Per quanto detto (e considerando anche il fatto che i SERT/SMI sono istituiti ai sensi di una legge speciale) per i servizi per le dipendenze è d'obbligo quindi anche informare preliminarmente gli interessati (preferibilmente per iscritto, a scanso di contestazioni), del diritto all'anonimato e delle conseguenze dell'una o dell'altra scelta. In particolare occorre chiarire che alle persone in anonimato non si potranno rilasciare certificazioni che, per definizione, richiedono l'identificazione. Si dovrà anche spiegare che, in caso di rinuncia all'anonimato, l'art. 92 del Codice consente, come illustrato più oltre, l'accesso alla cartella clinica nominativa anche a terze persone, anche contro la volontà dell'interessato, purchè intendano far valere diritti di pari grado anche in sede giudiziaria. Qualora il servizio utilizzi trattamenti informatizzati che comportino l'inserimento di dati anagrafici (come vedremo spesso non in linea con le disposizioni di legge, come dimostrano le numerosissime multe comminate dal Garante alla aziende sanitarie) l'interessato dovrà esserne informato. Gli si dovrà inoltre chiarire che la richiesta di anonimato non influirà in nessun modo sul diritto alla assistenza ambulatoriale ma, di fatto anche se non di diritto, potrebbe limitare le possibilità di accesso a strutture residenziali che richiedano il pagamento di una retta da parte dell'ente pubblico.
Sottolineiamo infine che, in assenza di precisazione nella informativa di eventuali finalità diverse da diagnosi e cura, il trattamento è illegittimo. In caso di un nuovo trattamento, con finalità diversa da quella precedente (per esempio una prestazione medico-legale per il conseguimento della patente), effettuato nei confronti dello stesso soggetto occorre quindi chiedere un nuovo consenso agli interessati per la nuova finalità o stabilire una nuova base giuridica.

Il trattamento dei dati epidemiologici nei Servizi per le Dipendenze

Come si è detto, l'art. 9 del Regolamento prevede la possibilità di trattare dati sanitari per "*motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri"* cioè sulla base di una legge o di una norma delegata da una legge. Per quanto riguarda le dipendenze il trattamento è previsto dall'art. 2, punto c del DPR 309 del 1990 che attribuisce al Ministero della Sanità (ora della Salute) la determinazione degli indirizzi per il rilevamento epidemiologico. Il Ministero è quindi intervenuto attraverso il D.M. 11 giugno 2010 che istituisce il Sistema Informativo Dipendenze (SIND). Tale sistema, si bassa sulla elaborazione di dati anonimi o anonimizzati, strettamente necessari alle finalità stabilite dalla legge. Non comprende quindi alcuna informazione sul Gioco d'Azzardo Patologico (GAP) né su dati giudiziari. Ciò in seguito al parere del 6 maggio 2009, in cui l'Autorità Garante chiedeva al Governo "*di espungere dallo schema la rilevazione di comportamenti come il gioco d'azzardo patologico e l'uso di tecnologie digitali che appaiono con evidenza eccedenti rispetto alle finalità del decreto il cui ambito di applicazione è la sola dipendenza da sostanze stupefacenti o da alcol anche in conformità a quanto previsto dalla normativa di settore"* e richiamava l'attenzione *"sulla circostanza che, allo stato, il ministero, le regioni e le province autonome non possono trattare tali dati per le finalità del presente*

decreto in quanto il loro trattamento non è previsto dai citati regolamenti sui dati sensibili e giudiziari per finalità di programmazione dell´assistenza sanitaria." . In seguito a ciò la possibilità di inserire nel sistema informativo dipendenze (SIND) il trattamento dei dati sul GAP è stata inserita in vari disegni di legge tra cui il testo unificato DDL S. 336 del 17 dicembre 2022 che ci risulta tuttora in attesa di approvazione. Un riferimento alla rilevazione dei dati è contenuto nell'allegato al D.M. 16 luglio 2021 n.136 ma senza alcun rimando alla legge che dovrebbe legittimarla. Notizie di stampa del dicembre 2022 riferiscono che un nuovo decreto in materia sarebbe all'esame del Garante. Tutto ciò considerato, visto che, in un recente passato, dati raccolti in difformità da quanto autorizzato per legge sono stati inseriti persino nelle relazioni annuali del Dipartimento Politiche Antidroga come "flusso extra SIND" senza indicare alcuna altra base normativa, suggeriamo ai responsabili del trattamento (in genere i Direttori di Struttura Complessa) di chiedere sempre alla autorità richiedente la base giuridica che giustifica la richiesta di dati.

Il consenso dell'interessato in Sanità e nei Servizi Tossicodipendenze

Oltre a stabilire all'art. 6 che il consenso dell'interessato è la prima base giuridica per il trattamento dei dati personali, salvo le eccezioni tassativamente indicate dalla legge, il GDPR stabilisce all'art. 7 le condizioni generali che lo rendono valido, precisando che sta al titolare "*dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali".* Come si è detto, prima che il trattamento dei dati abbia concreto inizio, è d'obbligo comunicare chiaramente all'interessato finalità, modalità del trattamento dei dati e diritti collegati in modo da consentirgli una decisone libera ed informata.
Con il citato provvedimento n. 55 del 7 marzo 2019 "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario",* il Garante ha tuttavia precisato che, diversamente dal passato e fermo restando l'obbligo di informazione, non è più necessario, nel quadro della nuova disciplina (art. 9, paragrafo 2 lettera h del GDPR), richiedere il consenso per i trattamenti dei dati per finalità di cura cioè *"quelli effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza."* Ciò indipendentemente dal fatto che si operi in libera professione o all'interno di strutture sanitarie. E' infatti evidente che, per il solo fatto di richiedere una prestazione sanitaria, si accetta anche di consentire il trattamento delle informazioni strettamente necessarie ad erogarla. Ciò però riguarda solo i dati *"essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute"* come da art. 53 del Regolamento mentre "*trattamenti attinenti, solo in senso lato, alla cura, ma non strettamente necessari",* anche se effettuati da professionisti della sanità, richiedono una distinta base giuridica. Pertanto il consenso è ancora richiesto, ad esempio, per alimentare il fascicolo sanitario elettronico, per la refertazione on line, per l'utilizzo di app o posta elettronica. E' necessario il consenso anche per i dati trattati attraverso dossier sanitario elettronico (trattamento informatizzato che fa capo ad un unico titolare) anche se il Garante si riserva di "*individuare nell'ambito delle misure di garanzia da adottarsi sulla base dell'art. 2-septies del Codice, i trattamenti che, ai sensi dell'art. 9, par. 2, lett. h), possono essere effettuati senza il consenso dell'interessato."*
Per il trattamento di dati soggetti a maggior tutela, come quelli riguardanti le dipendenze, è quindi consigliabile acquisire un consenso scritto ricordando che il comma 2 del citato art 7 dispone che se la dichiarazione scritta riguarda diverse questioni (per esempio il trattamento di dati a fini diversi come diagnosi e terapia o ricerca scientifica o la autorizzazione a comunicazione a diversi soggetti) "*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".* In caso contrario, nessuna parte della dichiara-

zione è vincolante. L'interessato inoltre "*ha il diritto di revocare il proprio consenso in qualsiasi momento"* ma "*la revoca del consenso non pregiudica la liceità del trattamento precedente"* e ed anche di ciò occorre dare informazione. Inoltre nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità che "*la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto."* In sintesi se un paziente richiede un certo trattamento (per esempio la disassuefazione da oppiacei) non è legittimo estorcergli il consenso al trattamento di dati non necessari a quella specifica prestazione come, ad esempio, quelli relativi le sue condizioni famigliari o sociali o i suoi precedenti penali.

Casi di emergenza

In base all'art. 82 del Codice l'informativa può essere resa anche dopo la prestazione:

- in caso di emergenza sanitaria o di igiene pubblica per cui sia stata emessa un'ordinanza dalle autorità sanitarie competenti (esempio: epidemia);
- quando l'interessato è in stato di incapacità e non è possibile acquisire il consenso dall'esercente la potestà, da prossimi congiunti, famigliari, conviventi o dal responsabile della struttura in cui dimora l'interessato (esempio: trattamento dei dati necessari al ricovero di persona trovata in stato di incoscienza);
- quando sussiste un rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato (esempio: necessità di identificare attraverso una banca dati il paziente a cui è stato consegnato un farmaco controindicato);
- tutte le volte che le procedure per l'acquisizione del consenso pregiudicherebbero l'efficacia di una prestazione medica.

Limitazioni alla conservazione e al trattamento dei dati personali

L'art. 5 lettera e) del GDPR dispone che i dati personali debbano essere conservati "*in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati"* e che "*possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici"*.
Una volta soddisfatta la finalità per cui sono stati raccolti in base ad una norma di legge o all'autorizzazione dell'interessato i dati dovrebbero quindi essere cancellati oppure resi anonimi. In questo caso, essendo impossibile la identificazione degli interessati, la normativa in materia di protezione dei dati personali non si applica. Ricordiamo però che l'identificazione potrebbe avvenire anche attraverso informazioni diverse da quelle anagrafiche. Per esempio in una raccolta di casi clinici "anonimi" alcune informazioni relative alla storia del paziente potrebbero comunque renderlo riconoscibile ai suoi famigliari o ai colleghi.

Diversa dalla anonimizzazione è la pseudonimizzazione che consiste nell'attribuire al soggetto un numero, pseudonimo o sigla che lo rendano non immediatamente identificabile ma che consentano però di risalire alle generalità attraverso una corrispondenza conservata separatamente. In questo caso si applicano tutte le disposizioni del GRPR e del Codice, comprese quelle relative alla conservazione. Per quanto riguarda i servizi per le dipendenze le disposizioni riguardanti la conservazione dei dati possono essere rilevanti per esempio per la valutazione a lungo termine della efficacia dei programmi che necessita di rilevarne l'esito anche a distanza di anni. E' perciò consigliabile chiedere all'apertura o alla chiusura della cartella clinica anche una separata autorizzazione a contattare la persona

(e quindi a conservare/utilizzare i suoi dati personali) dopo la chiusura del programma per questa specifica finalità.
Un particolare tipo di trattamento è la compilazione della cartella clinica. Questo documento si configura infatti come una registrazione di dati a cui la giurisprudenza ha più volte riconosciuto valore di atto pubblico e quindi, a differenza di quanto avviene in tutti gli altri casi, deve contenere, oltre ai dati raccolti dall'anamnesi e quindi riferiti dal paziente, tutto quanto il medico constata, purchè pertinente alla diagnosi e/o terapia, anche nel caso che l'interessato si opponesse alla registrazione. Se per esempio il paziente chiedesse di non segnalare in cartella l'esito positivo di un test infettivologico il medico dovrebbe ugualmente registrarlo. Proprio per la sua natura di atto pubblico, inoltre, la cartella clinica deve essere conservata illimitatamente e nulla di quanto contenutovi, anche se errato, può essere cancellato.

Statistica e ricerca scientifica

Il trattamento di dati sanitari per motivi di archiviazione nell'interesse pubblico, di ricerca scientifica o storica o a fini statistici è previsto dagli artt. 9 e 89 del GDPR purchè strettamente necessario agli scopi dichiarati e sempre sulla base del diritto europeo o degli stati membri. La questione è regolata in Italia dagli articoli 104-110 bis del Codice. Il trattamento dei dati a questi fini presuppone sempre che l'interessato venga informato sugli scopi della ricerca. Se un soggetto può rispondere in nome di un altro (per esempio nel caso di indagini riguardanti la famiglia) l'informazione può essere data attraverso la persona che risponde. L'informativa non è dovuta se richiede risorse sproporzionate al diritto tutelato ma, in questo caso, l'iniziativa deve essere adeguatamente pubblicizzata.
L'art. 106, in ogni caso, impegna il Garante promuovere la sottoscrizione di codici di deontologia e di buona condotta per i soggetti pubblici e privati, comprese società scientifiche ed associazioni professionali. Di regola la partecipazione a tali ricerche richiede il consenso degli interessati specie nei casi si trattamento di dati sanitari.
In base all'art.110 del Codice "*il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a norme di legge o quando informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca."* Anche in questi casi, però, il programma di ricerca deve ottenere non solo il parere' favorevole del competente comitato etico territoriale (come tutte le altre ricerche) ma deve anche essere sottoposto a preventiva consultazione del Garante, come previsto dall'articolo 36 del Regolamento.
Per quanto riguarda i ricercatori operanti in università, altri enti o istituti di ricerca e società scientifiche, al di fuori dal sistema statistico nazionale o da altre ricerche previste da norme nazionali o europee, la ricerca biomedica, rispetto al trattamento dei dati, deve essere svota secondo le "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica" pubblicate nella Gazzetta Ufficiale del 14 gennaio 2019, n. 11 a cui rimandiamo.
Per quanto riguarda le ricerche condotte in ambito assistenziale, infine, ricordiamo che richiedono in ogni caso (compresi gli studi osservazionali) il parere positivo del Comitato Etico, anche rispetto alla normativa sulla protezione dei dati personali.

Registro dei trattamenti e sicurezza dei dati

L'art 30 del GDPR obbliga ogni titolare a tenere un registro dei trattamenti svolti sotto la propria responsabilità. Il registro deve contenere una serie di informazioni tra cui finalità

del trattamento; categorie di interessati e di dati personali trattati; categorie di destinatari di eventuali comunicazioni; descrizione generale delle misure di sicurezza adottate.
Lo stesso obbligo riguarda i responsabili per i trattamenti di loro competenza.
Il citato provvedimento del Garante n. 55 del 7 marzo 2019 “Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario” conferma l’obbligo anche per le strutture sanitarie compresi i professionisti privati di dotarsi di tali registri. Si ricorda che per trattamento si intende “*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione”.* A mero titolo di esempio, ricordiamo che il professionista SERT che, di sua iniziativa, si crea una personale raccolta cartacea che tiene in un cassetto della propria scrivania con dati concernenti persone identificabili, magari con appunti personali relativi a terapie o psicoterapie, sta effettuando un trattamento illegittimo che viola sia numerose disposizioni di legge sia i Codici Deontologici.
L’art. 32 del GDPR stabilisce una serie obblighi, sia per il titolare sia per i responsabili, rispetto alla sicurezza dei dati, indicando anche la adozione di misure come pseudonimizzazione e cifratura dei dati personali; capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi, di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; presenza di una procedura per testare regolarmente l'efficacia delle misure adottate. Sono inoltre tenuti a far sì che *“chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento”.*

Rapporti con le norme deontologiche

Il CDM fa riferimento all'obbligo di trattare i dati personali e sensibili solo previo consenso informato dell'interessato e al divieto di collaborare alla costituzione o all'utilizzo di banche dati in assenza di garanzie su acquisizione del consenso e sicurezza agli artt. 12 e 13. Rispetto alle pubblicazioni scientifiche di dati clinici o di osservazioni relative a singole persone, il codice di deontologia medica fa obbligo al medico di assicurare la non identificabilità delle stesse e di non diffondere, attraverso la stampa o altri mezzi di informazione, notizie che possano consentire la identificazione del soggetto. Analoghe disposizioni sono contenute nei Codici Deontologici delle altre professioni già citate.

Test psicoattitudinali e definizione della personalità

L’articolo 22 del GDPR dispone che nessuno può essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (esempio test psicologici automatizzati) che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. In ogni caso l’interessato può opporsi ad ogni decisione basata sul trattamento automatizzato dei dati personali (salvo casi particolari come l’esecuzione di un contratto).

La comunicazione dei dati sanitari

I dati personali idonei a rivelare lo stato di salute dovrebbero essere resi noti all’interessato (o a chi ne ha la rappresentanza legale oppure ad un prossimo congiunto in

caso di incapacità di agire o di incapacità di intendere o di volere) solo da un medico o dal professionista che li ha trattati.
Riguardo ai Servizi Sanitari, salvo i già citati casi di "*giusta causa*" di rivelazione del segreto professionale, la comunicazione a terzi può avvenire solo se espressamente autorizzata dall'interessato. Non è quindi legittimo, per esempio, che un Ser.T. effettui una ricerca di follow-up chiedendo informazioni ad altre strutture sanitarie o, peggio, a comuni, parenti, datori di lavoro.

Altre misure per il rispetto dei diritti dell'interessato

Il Garante per la protezione dei dati personali, in seguito a "*reclami e segnalazioni con i quali si rappresentava che alcune strutture sanitarie, nell'erogare prestazioni e servizi per finalità di prevenzione, diagnosi, cura e riabilitazione, non rispetterebbero le garanzie previste dalla legge a tutela, in particolare, della dignità e della riservatezza delle persone interessate"* con suo provvedimento 9 novembre 2005 "*Strutture sanitarie: rispetto della dignità",* ribadiva che una serie di misure organizzative *"devono essere adottate per espresso obbligo di legge da tutti gli organismi sanitari, sia pubblici (es. aziende sanitarie territoriali, aziende ospedaliere), sia privati (es. case di cura)"* e che, tra l'altro, gli organismi sanitari pubblici e privati, in qualità di titolari del trattamento dei dati personali, devono garantire il rispetto dei principi, per quanto pertinenti, esplicitati nel Codice, che di seguito riassumiamo precisando che nel testo originale il Garante fa riferimento all'abrogato art 83 del Codice ora sostituito da una serie di diposizioni contenute o implicite nel GDPR.

a) Dignità dell'interessato **-** La prestazione medica e ogni operazione di trattamento di dati personali deve avvenire nel pieno rispetto della dignità dell'interessato La tutela della dignità personale deve essere garantita nei confronti di tutti i soggetti cui viene erogata una prestazione sanitaria, con particolare riguardo a fasce deboli quali i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno. La dignità deve essere garantita anche in caso di presenza di studenti autorizzati. In questo caso il paziente deve esserne informato, si devono adottare specifiche cautele volte a limitare l´eventuale disagio limitando ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie.
b) Riservatezza nei colloqui e nelle prestazioni sanitarie – Necessarie idonee cautele in relazione allo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi.
e) Distanza di cortesia - Le strutture sanitarie devono predisporre apposite distanze di cortesia in tutti i casi in cui si effettua il trattamento di dati sanitari (es. operazioni di sportello, acquisizione di informazioni sullo stato di salute), nel rispetto dei canoni di confidenzialità e della riservatezza dell'interessato.
f) Ordine di precedenza e di chiamata – Nelle sale d'aspetto l'ordine di precedenza e di chiamata degli interessati deve prescindere dall'uso dei nomi (ad es., attribuendo un codice numerico).
g) Correlazione fra paziente e reparto o struttura - Si devono adottare specifiche procedure, anche di formazione del personale, per prevenire che estranei possano dedurre lo stato di salute del paziente attraverso la correlazione tra la sua identità e l'indicazione della struttura o del reparto.

Le procedure che prevedono, per esempio, la somministrazione di farmaci contemporaneamente a più pazienti nello stesso locale, l'attesa in sale promiscue con altri

servizi sociali o sanitari, la chiamata nominale degli interessati, l'indicazione all'esterno del tipo di patologia trattata (Centro AIDS, Servizio Alcologia), l'esecuzione di prelievi urinari con porte aperte sono perciò illegittime e sanzionabili.

Utilizzo di videocamere

L'uso di videocamere è stato oggetto di uno specifico "Provvedimento in materia di videosorveglianza", 8 aprile 2010, da parte del Garante. Tale provvedimento si occupa specificamente di ospedali e luoghi di cura al punto 4.2 limitando *"l'eventuale controllo di ambienti sanitari (…) ai casi di comprovata indispensabilità, derivante da specifiche esigenze di cura e tutela della salute degli interessati"* pena l'applicazione di sanzioni amministrative. Solo in seguito, con Provvedimento 15 maggio 2013 n. 243, il Garante autorizzava l'uso di videocamere per la raccolta di campioni di urine se indispensabili a fini certificatori e clinici (ovviamente da dimostrare) a condizione che: all'interessato sia data facoltà di scelta tra ripresa con videocamera ed osservazione diretta; le immagini non siano registrabili; il servizio igienico sia adibito in via esclusiva a tali controlli; l'abilitazione a visionare le immagini sia riservata a personale sanitario incaricato per iscritto, preferibilmente dello stesso sesso delle persone controllate.

Banche dati e sistemi informatici e telematici

Data la velocità con cui si sviluppano nuove tecnologie il GDPR non entra nei particolari delle tipologie di banche dati e sistemi informatici e telematici utilizzabili ma all'art. 35 fa obbligo al titolare di effettuare, in ogni caso, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, consultandosi con il responsabile della protezione dei dati. La valutazione è richiesta in particolare per i dati citati nell'art. 9 compresi quelli sanitari e deve contenere almeno una descrizione dei trattamenti e delle loro finalità; una valutazione della necessità e proporzionalità dei medesimi; una valutazione dei rischi per i diritti e le libertà degli interessati; le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati.
Per quanto riguarda gli enti pubblici la norma tecnica di riferimento, anche per la riservatezza dei dati, è il Codice della Amministrazione Digitale a cui si rimanda.
La spinta per la sanità digitale appare tuttavia particolarmente rischiosa per la sicurezza dei dati in particolare per quelli (come l'uso di alcol e droghe) la cui conoscenza da parte di terzi potrebbe comportare danni per il singolo e per la società (si pensi ai casi di ricatto nei confronti di soggetti titolari di posizioni pubbliche). Tanto che una prima proposta di decreto sul cosiddetto Ecosistema Dati Sanitari presentato congiuntamente dai ministeri della Salute, dell'Economia e dal Ministro delegato per l'innovazione tecnologica e la transizione digitale è stato respinto con provvedimento del Garante n. 295 del 22 agosto 2022.
Da tutto ciò si evince che è assolutamente sconsigliato utilizzare nei servizi soluzioni informatiche faidate come è spesso avvenuto in passato.

Carte sanitarie elettroniche, fascicolo sanitario elettronico, dossier sanitari, referti on-line

L'articolo 59, comma 50, lettera i della legge 27 dicembre 1997, n. 449 e la legge 26 febbraio 1999 n. 39 prevedono l'utilizzazione di carte sanitarie elettroniche, cioè di tessere elettroniche che possono contenere i dati sanitari di un singolo individuo. Negli ultimi anni tuttavia si è diffusa un'altra e diversa forma di trattamento dei dati sanitari attraverso banche dati gestite da uno o più titolari in forma di dossier sanitario elettronico (DSE) e

fascicolo sanitario elettronico (FSE). Si tratta, in sintesi, della "*condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica.*" Per regolamentare tali processi il Garante emanò fin dal 16 luglio 2009 le *"Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario".* Il Garante definisce "*dossier*" un documento elettronico costituito da un unico titolare (per esempio ospedale o clinica privata) a cui accedano più professionisti. Mentre per "*fascicolo sanitario elettronico*" si intende il fascicolo formato con dati sanitari originati da diversi titolari.
Con propria delibera 4 giugno 2015 pubblicata sulla Gazzetta Ufficiale del 17 luglio 2015 il Garante ha emanato ulteriori Linee guida in materia di dossier sanitario resesi necessarie in seguito a numerose segnalazioni di violazione della normativa, riguardanti in particolare accessi abusivi ai dossier sanitari aziendali da parte di personale amministrativo e di personale medico che non era mai stato coinvolto nelle attività di cura. In tale documento (che invitiamo a consultare direttamente sul sito del Garante) si ribadiscono le indicazioni già contenute nelle linee guida del 2009 integrandole con ulteriori specificazioni in particolare riguardo ali contenuti dell'informativa, alla effettiva libertà del consenso e della sua revoca, al diritto all'oscuramento e alla visione degli accessi al proprio dossier da parte dell'interessato, precisando che l'amministrazione vi deve dare riscontro entro 15 giorni dalla richiesta elevabili a 30 in caso di particolare complessità tecnica. Il capitolo 3.1 è dedicato ai particolari casi di consenso riguardanti i soggetti a maggior tutela ivi compresi coloro che fanno uso di sostanze stupefacenti o psicotrope e di alcol. A questo proposito richiamiamo l'attenzione sul fatto che anche le informazioni sull'uso di alcol, spesso banalizzate o, addirittura, registrate in base a valutazioni del terapeuta a dispetto di opposte asserzioni dell'interessato, rientrano invece nei dati meritevoli di speciale protezione e autorizzazione. Infine il documento si sofferma sulla necessità di prevedere, nel rispetto del principio di indispensabilità dei dati, accessi modulari al dossier in base al tipo di prestazione che l'operatore deve fornire e sull'obbligo tassativo, la cui violazione configura illecito penale, i di designare nominativamente gli incaricati del trattamento indicando con chiarezza cosa ciascuno è autorizzato a conoscere e a fare.
Non ci sono stati invece ulteriori provvedimenti normativi del Garante per quanto riguarda il Fascicolo Sanitario Elettronico nazionale che è stato adottato ai sensi dell'art. 12 del Decreto Legge (DL) 179/2012 convertito con legge 221/2012 e dell'art 13, comma 2 quater del DL 69/2013 Tale decreto indusse infatti una serie di osservazioni del Garante, espresse con lettera al Ministro della Salute del 9 luglio 2013, che furono poi recepite nella legge di conversione 98/2013. Dopo parere positivo del Garante espresso con provvedimento n. 261 del 22 maggio 2014, è stato in seguito emanato con DPCM 29 settembre 2015 n. 178 il "Regolamento in materia di fascicolo sanitario elettronico".
Al momento i cui scriviamo è in corso di pubblicazione sulla Gazzetta Ufficiale un nuovo Decreto del Ministero della Salute di concerto con il Sottosegretariato alla Innovazione Tecnologica e con il Ministero dell'Economia che contiene un nuovo regolamento e abroga il DPCM 178 ad eccezione dei Capi III e IV che rimangono in vigore fino alla emanazione di ulteriore decreto per l'utilizzo dei dati FSE a fini di ricerca e governo.
Il nuovo regolamento rende obbligatoria la costituzione del FSE in tutto il territorio nazionale recepisce le indicazioni del Garante e definisce, attraverso gli allegati, una serie di standard tecnici a cui adeguarsi, compresa la inter-operatività tra sistemi regionali.
Il FSE deve contenere i seguenti dati e documenti erogati anche al di fuori del Servizio Pubblico (art.3): dati identificativi ed amministrativi; referti; verbali di Pronto Soccorso; lettere di dimissione; prescrizioni ed erogazioni specialistiche e farmaceutiche a carico e non del Sistema Sanitario; vaccinazioni; lettere di invito per screening. Contiene inoltre un

profilo sanitario sintetico che dovrà essere redatto dal medico di base (art 4) e un taccuino personale dell'assistito dove l'interessato potrà inserire dati anamnestici non certificati (art. 5). Entro tre mesi dall'entrata in vigore del provvedimento Ministero della salute e Regioni dovranno fornire all'interessato una informativa su modello nazionale con quanto previsto dagli artt. 13 e 14 del GDPR (art.7). L'assistito, dopo aver preso visione dell'informativa potrà esprimere un consenso (o un dissenso) *"libero, specifico, informato ed inequivocabile"* e disgiunto alla consultazione dei dati da parte di operatori sanitari per le diverse finalità di cura, prevenzione e profilassi internazionale. Il consenso potrà essere revocato in qualsiasi momento ma i dati non verranno cancellati ma rimarranno consultabili dall'interessato e da chi li prodotti. I dati soggetti a maggior tutela tra i quali l'uso di alcol e droghe, *"sono resi visibili solo all'assistito*" che può decidere di renderli visibili a terzi rilasciando "*esplicito, informato e specifico consenso"* al soggetto che eroga la prestazione. Solo nel caso di richiesta di anonimato il FSE non va alimentato (art.6). Devono infatti essere rispettate le disposizioni relative al diritto all'anonimato previste per le vittime di atti di violenza sessuale o di pedofilia (l. 15 febbraio 1996, n. 66; l. 3 agosto 1998, n. 269 e l. 6 febbraio 2006, n. 38), delle persone sieropositive (l. 5 giugno 1990, n. 135), di chi fa uso di sostanze stupefacenti, di sostanze psicotrope e di alcool (D.P.R. 9 ottobre 1990, n. 309), delle donne che si sottopongono a un intervento di interruzione volontaria della gravidanza o che decidono di partorire in anonimato (l. 22 maggio 1978, n. 194; d.m. 16 luglio 2001, n. 349), nonché con riferimento ai servizi offerti dai consultori familiari (l. 29 luglio 1975, n. 405)

L'interessato ha il diritto di oscurare singoli dati al momento della alimentazione del FSE facendone richiesta direttamente a chi eroga la prestazione che ha il dovere di informarlo di questa possibilità. L'oscuramento può essere richiesto o revocato in qualsiasi momento anche tramite apposita funzionalità on line e comporta che i soggetti abilitati ad accedere ai dati per finalità di cura non vengano a conoscenza che i dati oscurati esistono (oscuramento dell'oscuramento, art. 9). Il titolare del trattamento è tenuto alla conservazione dei dati per 30 anni dopo il decesso dell'interessato ad eccezione della cartella clinica che va conservata in eterno (art.10). Per quanto riguarda minori e incapaci il rilascio del consenso ed i diritti relativi all'accesso e all'oscuramento devono essere esercenti dagli esercenti responsabilità genitoriale o tutela (artt. 8 e 11). Ciò appare in contrasto con le disposizioni dell'art. 120 del DPR 309/1990 in quanto stabilisce che nel caso di minori o incapaci la richiesta di presa in carico può essere diretta al SERT "anche" dai genitori o dal tutore. Ricordiamo ancora una volta che la legge speciale, come il DPR 309, prevale sulla legge ordinaria precedente o successiva e quindi non si potrà certo rifiutare di accogliere un minorenne perché non può dare il consenso al FSE. Rileviamo anche che l'art. 12 del nuovo regolamento indica tra i soggetti tenuti ad alimentare il FSE "*entro 5 giorni dalla erogazione della prestazione*" (comma 3) le strutture sanitarie pubbliche, accreditate e autorizzate, i servizi socio-sanitari regionali, gli esercenti le professioni sanitarie che operano in autonomia senza alcuna prevista eccezione per i SERT che dovranno quindi alimentare il FSE e per di più (comma 4) indicando per ogni dato inserito relativo alle dipendenze indicate nell'art. 6, se è stato o no esercitato il diritto all'oscuramento di cui all'art. 9. L'accesso ai dati per finalità di cura (art. 15), prevenzione (art. 16) o profilassi internazionale (art 19) è in ogni caso consentito solo a medici, infermieri, ostetriche, farmacisti e amministrativi con privilegi selettivi: ad esempio non è consentito all'infermiere consultare un referto di laboratorio né al farmacista consultare una scheda di vaccinazione che invece è accessibile all'infermiere.

In caso di emergenza e di incapacità fisica o psichica a fornire il consenso è consentito l'accesso al FSE se le informazioni sono indispensabile a cure salvavita e per il tempo strettamente necessario ad erogarle con l'esclusione dei dati oscurati. (art 20).

Gli accessi al FSE devono essere registrati e l'interessato deve poterne prendere visione tramite apposita funzionalità. Inoltre le Regioni dovranno fornire un sistema di notifica degli accessi via posta elettronica o tramite app mobile (art 22).
Infine all'art 25 il Decreto fornisce indicazioni tassative sulla misure di sicurezza che devono essere adottate.

Comunicazioni via e-mail, via sms, via messaggerie, via fax o telefoniche

Le comunicazioni on line non danno garanzia assoluta di riservatezza. Il Garante ha affrontato la problematica dei referti on line con le Linee guida in tema di referti on-line - 19 novembre 2009. In tale documento si fa riferimento anche alla modalità di invio presso caselle postale elettronica indicata dall'interessato. A queste indicazioni ci si può attenere anche per altre comunicazioni. In particolare si raccomandano le seguenti precauzioni:
1. spedizione del referto in forma di allegato a un messaggio *e-mail* e non come testo compreso nella *body part* del messaggio;
2. il file contenente il referto dovrà essere protetto con modalità idonee a impedire l´illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati (*password* per l´apertura del file o chiave crittografica comunicate per altro canale). Tale cautela può non essere osservata qualora l´interessato ne faccia espressa e consapevole richiesta, in quanto l´invio del referto alla casella di posta elettronica indicata dall´interessato non configura un trasferimento di dati sanitari tra diversi titolari del trattamento, bensì una comunicazione di dati tra la struttura sanitaria e l´interessato effettuata su specifica richiesta di quest´ultimo;
3. convalida degli indirizzi *e-mail* tramite apposita procedura di verifica *on-line*, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall´utente richiedente il servizio.
Per il professionista vale in ogni caso l'obbligo di tutelare il segreto professionale qualunque mezzo utilizzi ricordando che nessuno dei mezzi sopracitati, nella versione gratuita dà assolute garanzie di riservatezza. Il sito del GDPR indica tuttavia i servizi ritenuti più in linea con le proprie indicazioni.
Particolarmente pericolose sono le segreterie telefoniche sulle quali un troppo fiducioso cittadino potrebbe lasciare informazioni riservate non sapendo che, per esempio, vengono in quel momento ascoltate da addetti alle pulizie, tirocinanti, elettricisti, centralinisti, amministrativi o quant'altri abbiano accesso ai locali. E' pertanto compito del dirigente responsabile della struttura dare disposizioni affinchè chi lascia messaggi sulla segreteria del servizio venga avvertito con un messaggio registrato che non ne è in alcun modo garantita la riservatezza. Nessun operatore dovrebbe lasciare messaggi atti a rivelare dati sensibili (compresa la frequenza a servizi o reparti che di per sé indicano la patologia trattata) su nessuna segreteria. Le stesse considerazioni valgono per quanto riguarda i fax non criptati che dovrebbero essere limitati ai casi di assoluta necessità e, in ogni caso, dovrebbero essere immediatamente preceduti da telefonata per garantirsi che la persona a cui sono diretti sia lì a riceverli. Per quanto riguarda psicoterapie o altre comunicazioni on-line è fondamentale che l'interessato venga invitato a non usare mai nè il proprio nome o cognome, né un account che lo contenga o lo suggerisca. Inoltre non dovranno mai essere citati nomi e cognomi di terze persone. E' sconsigliabile, in ogni caso, fare riferimento diretto a fatti o diagnosi che l'interessato voglia mantenere segrete. Nelle comunicazioni via sms non vanno mai citati espressamente dati sensibili dato che sia il cellulare del terapeuta che quello del paziente potrebbero facilmente finire in altre mani per smarrimento o furto. Il terapeuta dovrebbe in ogni caso mantenere l'accesso al telefono con password e tenerlo chiuso quando non l'avesse con sé. Non dovrebbe mai

utilizzare nella rubrica cognomi e nomi ma solo sigle. Anche la rubrica di un cellulare ad uso professionale è infatti un trattamento di dati personali.

La cartella clinica socio-sanitaria nei Servizi Tossicodipendenze

Come si è visto, il fascicolo sanitario elettronico dovrebbe contenere anche le cartelle cliniche che, come tali, a differenza delle altre componenti, devono essere conservate in eterno. Questa disposizione, allo stato attuale, crea una serie di problemi specifici per i servizi per le dipendenze che dovrebbero essere attentamente considerati.
Precisiamo che non esiste una normativa specifica riguardante la cartella clinica.
L'unico riferimento normativo è rintracciabile, a tutt'oggi, nelle "Linee guida 17 giugno 1992- La compilazione, la codifica e la gestione della scheda di dimissione ospedaliera istituita ex DM 28-12-1991" del Ministero della Sanità che definiscono la cartella clinica come *«il chi, cosa, quando, come e perché dell'assistenza al paziente».*
Anche in mancanza di indicazioni di legge, una costante giurisprudenza ha però definito la cartella clinica**,** se redatta da addetto a pubblico servizio, come atto pubblico di fede privilegiata.
L'atto pubblico è il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è formato. Nella giurisprudenza la figura dell'addetto a pubblico servizio (identificato con chiunque stia espletando funzioni che rappresentano la volontà della pubblica amministrazione) è di fatto assimilata a quella del pubblico ufficiale. Perciò gli atti prodotti da dipendenti o convenzionati o in altro modo aggregati al SSN hanno valore di atto pubblico.
La cartella clinica socio-sanitaria dei Servizi Pubblici per le Tossicodipendenze è il fascicolo in cui si raccolgono i dati anamnestici e obbiettivi riguardanti il paziente, quelli sul decorso della malattia, i risultati degli accertamenti e delle terapie praticate. E' un documento, quindi, nel quale si esprime e si manifesta l'attività dell'ente e che, oltre a rappresentare uno strumento di lavoro, ha rilevanza giuridica perché non persegue solo finalità pratiche e statistiche di ordine interno ma consacra una determinata realtà (visite, natura e gravità della malattia, terapia) che può essere fonte di diritti ed obblighi per lo Stato e per lo stesso paziente. Si pensi ad esempio al trattamento di tossicodipendenti in regime di sospensione della pena detentiva oppure ai lavoratori tossicodipendenti che possono richiedere l'aspettativa per effettuare programmi terapeutici, o a chi richiede una certificazione per riottenere la patente di guida. Sono solo alcune delle fattispecie nelle quali la documentazione del Ser.T. rappresenta una prova documentale, sancita anche dal D.M. n. 186 del 12 luglio1990 laddove all'art. 1, tra le procedure diagnostiche e medico-legali per l'accertamento dell'uso abituale di sostanze psicotrope, viene citato il riscontro documentale di trattamenti socio-sanitari per le tossicodipendenze. Per questi motivi la giurisprudenza della Suprema Corte, chiamata a pronunciarsi in tema di falsità in atti, ha ritenuto in varie sentenze che la cartella clinica, redatta da un sanitario esercente un pubblico servizio, costituendo autonoma prova del corretto adempimento dei doveri di una pubblica amministrazione in riferimento ai diritti del malato o di terzi, è atto pubblico di fede privilegiata, la cui falsificazione porta all'applicazione degli articoli 476 e 479 del CP riguardanti il falso materiale e il falso ideologico. Come atto pubblico, quindi, la cartella clinica è un bene patrimoniale indisponibile (art. 830 Codice Civile, d'ora in poi CC) e pertanto, quanto alla sua conservazione, è soggetto al regime generale dei beni pubblici come già stabilito dall'art. 8 del DPR 30 settembre 1963 n. 1409 sugli Archivi di Stato e confermato dal D. Lgs. 42/2004 "Codice dei beni culturali e del paesaggio". Il ritardo nella sua compilazione potrebbe comportare la sussistenza del reato di omissione di atti d'ufficio, punibile ai sensi dell'art. 328 CP e l'annotazione postuma di un fatto clinico rilevante integra il reato di falso materiale di cui all'art. 476 del CP.

La cartella clinica acquista il carattere di definitività in relazione ad ogni singola annotazione che quindi esce dalla sfera di disponibilità del compilatore non appena viene riportata. Le modifiche o aggiunte ad un atto pubblico dopo che è stato definitivamente formato integrano il falso anche se il soggetto ha agito per ristabilire la verità effettuale, in quanto, a causa dell'aggiunta postuma, l'atto viene a rappresentare e documentare fatti diversi da quelli che rappresentava e documentava nella versione originale. Eventuali errori, pertanto, non devono essere corretti cancellandone le tracce o, peggio, rifacendo la cartella ma devono essere rettificati con la data del momento in cui l'annotazione correttiva è stata redatta.
Una versione informatica della cartella clinica è prevista dall'art. 47 bis della legge 4 aprile 2012 n. 35 che dispone che *"nei piani di sanità nazionali e regionali si privilegia la gestione elettronica delle pratiche cliniche, attraverso l'utilizzo della cartella clinica elettronica".* Dati i risvolti di tipo legale sopra illustrati, la cartella clinica elettronica dovrebbe avere le stesse caratteristiche di attribuibilità certa delle diverse annotazioni, integrità, non modificabilità, possibilità di estrazione di copie distinguibili dall'originale delle cartelle cartacee, attribuibilità certa delle diverse annotazioni con disponibilità per ogni operatore della firma digitale.
Il citato Codice Amministrazione Digitale dispone all'art. 22 che un documento informatico *"ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalita' tali da garantire la sicurezza, integrita' e immodificabilita' del documento e, in maniera manifesta e inequivoca, la sua riconducibilita' all'autore."*
Purtroppo non pochi dei numerosi software diffusi nei SERT sotto il nome di cartella clinica informatizzata non solo non rispondono ai requisiti previsti per un atto pubblico digitale, ma spesso non rispettano nemmeno le indicazioni di legge per la gestione dei dossier sanitari elettronici. Anche nel caso ci si avvalesse di un dossier sanitario elettronico in regola con la vigente normativa (strumento peraltro alimentabile solo con il libero consenso dell'interessato che non deve subire alcuna riduzione delle prestazioni in caso di non adesione) non viene meno l'obbligo di compilare una cartella clinica con i requisiti richiesti da un atto pubblico.
Un ulteriore problema spesso poco considerato riguarda la effettiva segretezza della cartella clinica del SERT.
Il paziente titolare della cartella, cartacea o informatizzata, ha in ogni momento accesso al suo contenuto ed era, fino al 31 dicembre 2003, l'unico soggetto titolato a chiederne copia con le uniche eccezioni degli eredi legittimi, del rappresentante legale della persona minore o dichiarata legalmente incapace e, in certi casi, delle compagnie di assicurazioni. L'art. 92 del Codice ha introdotto la possibilità di accedere alla cartella clinica, o all'acclusa scheda di dimissione ospedaliera, anche ad altri soggetti diversi da quelli sopra citati, a fronte di una documentata necessità

1) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'art. 26 comma.4 (che indica i casi eccezionali in cui è ammissibile il trattamento di dati sensibili anche senza il consenso dell'interessato, previa autorizzazione del garante) di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
2) di tutelare, in conformità alla disciplina sull'accesso agli atti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato.

Il succitato articolo 92 prevede anche il rilascio della cartella, "*in tutto o in parte*", a terzi legittimati.

L'entrata in vigore di questo articolo ha, di fatto, aperto una nuova problematica. Con suo provvedimento del 9 luglio 2003 "*Provvedimento generale sui diritti di pari rango*", infatti, il Garante precisava che per diritti di pari rango si intendono i diritti della personalità o "*altri diritti e libertà fondamentali in inviolabili*" collegati ad un "*elenco aperto di posizioni soggettive individuabile in chiave storico-evolutiva*". Inoltre la richiesta di accesso o di comunicazione di dati deve essere accolta quando "*sia formulata dal difensore ai sensi della disciplina sulle investigazioni difensive introdotta dalla legge n. 397/2000 e, in particolare, dell'art. 391-quater del codice di procedura penale."* In ogni caso, prima di rilasciare la copia, "*andrebbe interpellato l'interessato, per avviare un contraddittorio anticipato che può consentire a quest'ultimo, oltre alla tutela giurisdizionale in sede amministrativa, anche di opporsi per motivi legittimi al trattamento delle informazioni che lo riguardano"* presumibilmente negando che il diritto accampato sia di pari rango. Si potrebbe per esempio ritenere che i diritti e le libertà inviolabili siano quelli definiti tali dai titoli I e II e III della Costituzione tra cui il diritto alla salute definito nell'articolo 32. Potrebbe quindi verificarsi il caso che, per esempio, chi fosse venuto a contatto con persone sospettate di essere affette da malattie infettive o i cittadini in dubbio sulle condizioni psico-fisiche del proprio medico o, come è successo, il coniuge che intende ottenere l'annullamento del matrimonio anziché il divorzio utilizzando la patologia psichiatrica della moglie, chiedano, e ottengano, l'accesso alla cartella clinica dell'interessato sostenendo il proprio uguale diritto alla salute. Si è già verificato anche il caso di dover dare al difensore di un imputato per spaccio copia della cartella clinica di una paziente tossicodipendente che lo aveva denunciato. Tale normativa ha particolare rilevanza per i servizi e per i professionisti che si dedicano alla cura di patologie del comportamento. Si immagini, per esempio, a come potrebbe essere utilizzato ciò che un paziente confida ad uno psicoterapeuta, in una causa di separazione o per l'affidamento di un minore. Oppure alla richiesta di un datore di lavoro di accedere alla cartella clinica di un camionista dopo un incidente per procedere ad un licenziamento. Sembra di capire infatti che la cartella clinica perda sempre più la funzione di documento redatto per tutelare la salute dell'interessato e divenga comune atto pubblico utilizzabile da chiunque ne abbia interesse legittimo sebbene di particolare rango. In realtà il più volte citato articolo 120 del DPR 309/1990 che rinvia all'articolo 103 del CPP, in quanto norma di legge speciale, dovrebbe rappresentare una sufficiente tutela per le persone afferenti ai Servizi Tossicodipendenze. In base a ciò la magistratura, per esempio, può chiedere il sequestro delle cartelle cliniche di un Servizio Tossicodipendenze solo nei casi e nei modi indicati nello stesso art. 103: vietati anche alla magistratura perquisizioni, sequestro di documenti, intercettazioni telefoniche, sequestro o ogni forma di controllo della corrispondenza se non per accertare reati commessi dal personale o per cercare cose o persone specificamente determinate. Anche in questo caso ciò deve essere fatto personalmente dal giudice o dal pubblico ministero e solo alla presenza del presidente o di un consigliere dell'Ordine Professionale.
Tuttavia il rilascio di copia delle cartella compete alle Direzioni Sanitarie che, anche con il supporto degli Uffici Legali aziendali, in genere accolgono queste richieste.
Dato tutto quanto sopra esposto rispetto alla tutela della riservatezza, ed ai suoi limiti, sottolineiamo ancora una volta che il paziente deve essere chiaramente informato di queste possibilità prima di decidere se richiedere o meno l'anonimato dato che, allo stato dei fatti, questo è ad oggi il solo modo di mantenere davvero segrete le informazioni coperte dal segreto professionale.
Si ribadisce anche che, in ogni caso, la cartella clinica non deve in alcun modo contenere notizie relative a persone diverse dal paziente (tanto meno se tali notizie configurassero reati) se non come fatti riferiti e solo se pertinenti alla gestione del caso. Inoltre, dato che le notizie registrate devono essere quelle strettamente necessarie alla migliore gestione del caso, le informazioni sul paziente e sui famigliari dovranno essere riportate solo se

effettivamente indispensabili alla gestione dei problemi sanitari, psicologici e sociali su cui ci viene richiesto di intervenire. In conclusione, la cartella clinica deve rappresentare un documento e uno strumento di lavoro che contenga tutto quanto è necessario e sufficiente a svolgere nel modo migliore l'intervento che il paziente richiede ed autorizza, senza omissioni ma anche senza dati eccedenti.

Le sanzioni per chi viola la normativa sulla protezione di dati personali

Il GDPR prevede una serie di sanzioni per la violazione delle norme sulla protezione dei dati personali all'art 83 che (comma 4) possono arrivare fino al 4% del fatturato annuo dell'azienda. Ricordiamo che, in caso di aziende pubbliche, la Corte dei Conti procede poi per danno erariale per rivalersi nei confronti dei dirigenti o dipendenti pubblici responsabili delle violazioni di legge.
L'art.166 del codice attribuisce al Garante le competenze per irrogare le sanzioni e ne definisce i criteri.
Il procedimento (comma 4) puo' essere avviato, nei confronti di privati o di autorità ed organismi pubblici, in seguito a reclamo ai sensi dell'articolo 77 del GDPR o di iniziativa del Garante stesso.
In caso di danni gli interessati possono in ogni caso ricorrere alla magistratura civile per richiedere un adeguato risarcimento ai sensi dell'art. 2050 del Codice Civile.
Qualora ci sia dolo, gli artt. 167, 167 bis, 167 ter, 168, 170 e 171 del Codice prevedono invece sanzioni penali fino a 4 anni di reclusione per trattamento illecito di dati; comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala; acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala; falsita' nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante; inosservanza di provvedimenti del Garante; violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori.

Come rivolgersi al Garante

Le informazioni su come rivolgersi al Garante, nonché sulla la legislazione e la giurisprudenza aggiornate in materia e sulle iniziative in corso possono essere reperite sul sito internet

www.garanteprivacy.it

E' possibile rivolgersi direttamente al Garante ai seguenti recapiti:

Piazza Venezia n. 11 - 00187 Roma;
Centralino telefonico: (+39) 06.696771;
Fax: (+39) 06.69677.3785;
Posta elettronica: protocollo@gpdp.it;
PEC (solo da altra PEC): protocollo@pec.gpdp.it

Indice