

## Piano di Formazione Nazionale 2019

### Report Webinar n. 2 “Privacy: i dati sanitari”

**15 maggio 2019  
(11.00-13.00)**

Il giorno **15 maggio** si è svolto il secondo webinar organizzato da ProMIS nell’ambito del Piano di Formazione Nazionale per il 2019, a cui hanno partecipato all’incirca una cinquantina di persone.

La sessione ha visto il **prof. Paolo Guarda**, Facoltà di giurisprudenza di Trento, affrontare il tema della Privacy, nello specifico del trattamento dei dati sanitari, a seguito del più generale webinar tenutosi lo scorso febbraio. Per iniziare, il docente ha parlato dei cambiamenti nel rapporto medico-paziente a seguito del nuovo quadro normativo introdotto dal **DGPR UE 2016/679**, approvato in Italia nel maggio del 2018, in materia di trattamento dei dati personali; vi è poi il **D.lgs. 30 giugno 2003, n. 196** “Codice in materia di protezione dei dati personali”, recante disposizioni per l’adeguamento dell’ordinamento nazionale a questo nuovo regolamento, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE che colma ciò che non copre il GDPR. Il **D.lgs. 10 agosto 2018, n. 101** ha poi novellato il codice privacy chiarendo tutti i punti che avevano bisogno di maggior dettaglio a seguito dell’introduzione del DGPR. Il Garante Europeo va ad uniformare una disciplina frammentata, cercando dei compromessi tra i 28 Stati, in uno scenario in materia di trattamento dei dati per i quali gli stati membri hanno sempre avuto un ampio margine di discrezionalità. Chiarisce ed aggiorna inoltre la terminologia. Se si guarda all’attuale rapporto medico paziente, la tecnologia digitale ormai influenza tale relazione; il medico rielabora le informazioni in termini di diagnosi e ciò può essere visto come un’elaborazione di dati. Ad oggi il paziente è sempre più al centro della sua salute, come soggetto attivo che si informa, a volte non correttamente, ma che in ogni caso gioca un ruolo importante nella gestione dei propri dati.

I dati sanitari sono considerati **dati sensibili**: il legislatore europeo è molto attento a questa materia proprio per il passato storico di discriminazione che ha caratterizzato il secolo scorso (es. regime nazista).

Il concetto di dato sanitario era stato definito per la prima volta nella **Convenzione di Strasburgo 108/1981** «Sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale» e ripreso dalla **direttiva 95 del 1996** in cui il legislatore limita fortemente il trattamento di dati di questo tipo. All’art. 8, par. 1 si stabilisce che: «*Gli Stati membri vietano il trattamento di dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l’appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale*»; questa definizione viene poi ripresa dal D.lgs. 196/2003, ove i “*dati sensibili sono i dati personali idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l’adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*”, introducendo un elemento di elasticità e flessibilità. Esiste un dibattito su quale sia l’ambito di applicazione di tale definizione.

1. I dati sanitari sono solo quelli che rivelano malattie o anche le informazioni che lasciano intendere che possa sussistere un problema di salute?
2. Sono coperte solo le informazioni relative a condizioni attuali o anche a quelle pregresse?
3. Accento non sul tipo di dato, bensì sul contesto: 1. appunto, dato sanitario 2. rilevanza sia dei dati idonei a rivelare lo stato di salute che di quelli meramente di carattere amministrativo i quali risulterebbero così difficilmente separabili.

Nel contesto sanitario il trattamento del dato è particolarmente delicato, per questo il GDPR riprende e cerca di superare le incomprensioni dei contesti precedenti. Non si parla più di dati sensibili, ma di categorie particolari di dati e si fornisce **una definizione ad hoc** dei dati relativi alla salute a livello europeo che devono essere adottate da tutti gli Stati Membri. Si stabilisce all'art 4. che *“i dati relativi alla salute sono 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”*. Al n.35 si specifica poi che *“dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso”*, richiamando un contesto anche amministrativo dei dati sanitari. Vengono, inoltre, chiarite le **condizioni di legittimità** del trattamento, le quali obbligano ogni soggetto che interviene sui dati a giustificarne l'utilizzo. In questa cornice, il **consenso dell'interessato** legittima il titolare del trattamento a farlo. L'Art. 9, par. 1, GDPR disciplina le categorie particolari di dati personali: *«E' vietato trattare dati personali 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 una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»* con eccezioni come il consenso esplicito (lett. a); Trattamento necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (lett. c); Trattamento necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (lett. g); Trattamento necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero e altri. Il consenso è altresì una misura di garanzia introdotta dal GDPR. Ogni Stato Membro può poi introdurre eventuali condizioni per le misure di garanzia, già espresse dal garante, in maniera più sistematica ed omogenea.

Il Regolamento enfatizza il ruolo dei governi nazionali e del comitato dei garanti, cercando di favorire una soluzione generale per poi consentire, a livello nazionale, una declinazione più uniforme per quanto riguarda le misure di garanzia.

In Italia, il codice privacy è stato molto novellato; vengono previsti specifici **obblighi** come il rispetto dei principi di cui all'art. 5 del GDPR e altri, quali:

- ✓ Il soggetto titolare del trattamento deve valutare e documentare il processo decisionale e le misure poste in essere per poter poi giustificarle in sede di controllo (cd. responsabilizzazione del titolare trattamento);
- ✓ I dati vanno protetti sin dalla loro progettazione; è necessaria una corretta mappatura dei flussi e della governance dei ruoli;

- ✓ La **formazione** dei soggetti diventa elemento fondamentale. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità, e abbia accesso ai dati personali, non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;
- ✓ La **valutazione d'impatto** è una best practice obbligatoria (DPIA);
- ✓ Il registro delle attività è obbligatorio ed è uno strumento di cooperazione con le attività di controllo;
- ✓ La nomina del DPO, responsabile della protezione dei dati è altro elemento fondamentale e novità introdotta nel contesto italiano come obbligo: questo soggetto sarà un professionista esperto nella protezione dei dati, con il compito di valutare ed organizzare la gestione del trattamento dei dati personali all'interno di ciascuna organizzazione.
- ✓ Sussiste l'obbligo di nominare un DPO quando:
  1. Il trattamento è effettuato da autorità pubbliche o organismi pubblici (ad eccezione delle autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali);
  2. Il trattamento implica un monitoraggio su larga scala;
  3. Trattamento su larga scala di categorie particolari di dati personali e dati relativi a condanne penali e a reati.

L'art 15 del GDPR stabilisce poi i **diritti dell'interessato**: diritto di accesso, di rettifica, diritto alla cancellazione (diritto all'oblio), diritto di limitazione di trattamento, diritto di opposizione al trattamento.

Quali sono le **nuove sfide affrontate dal GDPR**: l'aumento e l'evoluzione della domanda di servizi socio sanitari, l'invecchiamento della popolazione, l'evoluzione dei sistemi di offerta dei servizi, l'aumento della mobilità di pazienti e del personale sanitario vengono considerate tali. Il trattamento dei dati caratterizzato dalle tecnologie digitali disumanizza il rapporto medico-paziente, ma è efficace per la sua interdisciplinarietà e migliora i sistemi sanitari.

Al termine della lezione si è aperta poi la sessione delle domande da parte dei partecipanti al webinar. Il dato sensibile non è un'informazione anonima: qualora sia necessario trattare dati personali, qualsiasi informazione riferibile ad un soggetto è considerata tale. Se l'informazione è sensibile, ma non agganciata al soggetto persona fisica, non è più collegata ad un soggetto e quindi non è più sensibile. Per definire quali siano i soggetti che in concreto nell'ambito della ricerca devono trattare i dati, è necessario effettuare una mappatura del contesto, definire le regole da applicare e delle linee guida, oltre ad eventuali responsabili e titolari. La ritenzione del dato è legata alla privacy ed è obbligatoria per altre finalità o interessi. Per questo motivo, un'azienda sanitaria ha obblighi di non trasferimento. Inoltre, la formazione del personale deve essere documentata per provare al Garante che si è fatto di tutto per prevenire il rischio della non corretta gestione del dato, pena la responsabilità civile del titolare del trattamento (responsabile della formazione e degli obblighi di accountability).