SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale della Romagna

Allegato n. 1

Linee guida per il trattamento e la tutela dei dati personali all'interno della AUSL della Romagna

Premessa

La tutela dei dati personali (c.d. privacy), coincidendo con la tutela della dignità e della libertà delle persone, è uno degli aspetti di cura della salute che l'Azienda USL della Romagna esercita con particolare attenzione e cura. Per questo motivo l'Azienda ha posto in essere una serie di azioni ed iniziative per uniformare tutte le attività e le relative strutture operative ai principi ed alle norme contenute nel D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" di seguito Codice Privacy, come innovato dal Regolamento Generale sulla Protezione dei Dati o Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, cosiddetto GDPR, concernente la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). e modificato e integrato dal D.Lgs. 101/2018.
L'intero impianto normativo, sia il primo del 1996 che il Codice del 2003, che il GDPR del 2016, si propone di tutelare il diritto alla riservatezza e alla protezione dei dati personali dei terzi siano questi i cittadini che accedono alle strutture dell'Azienda oppure operatori che vi lavorano.
Il presente regolamento ha l'obiettivo di rivisitare le precedenti Linee guida aziendali in materia di trattamenti dei dati, alla luce delle nuove disposizioni normative europee e nazionali soprarichiamate e rendere operative ed omogenee le stesse disposizioni in tutto l'ambito aziendale.
Il Titolare del trattamento ha nominato i Responsabili interni del trattamento dati, individuati in quei dirigenti (Direttori di struttura complessa, Responsabili di struttura semplice dipartimentale e Direttori di distretto) che hanno il compito di supportarlo nell'attuazione delle norme di garanzia della privacy all'interno del servizio, reparto o struttura da loro diretto in coerenza con le indicazioni di legge e aziendali.
L'elenco completo dei Responsabili interni del trattamento è consultabile sul WEB aziendale alla sezione "Privacy e tutela dati personali " e nella medesima sezione della intranet aziendale.
Tutti coloro che a diverso titolo operano in nome e conto dell'Azienda USL e che trattano dati personali di terzi sono designati "autorizzati" di trattamento dei dati personali, ricevono istruzioni operative e formazione specifica e sono chiamati al rigoroso segreto d'ufficio. Allo scopo di non tralasciare nessun professionista, dette nomine hanno luogo al momento stesso dell'inizio del rispettivo servizio e nello specifico, su espresso mandato del Titolare, al momento della sottoscrizione del rispettivo contratto individuale.
L'Azienda Usl della Romagna ritiene necessario assicurare continua attività formativa in materia, finalizzata a consolidare negli operatori la cultura del rispetto della dignità e della riservatezza nei confronti dei dati di terzi e, altresì, approfondire con gli operatori le indicazioni del Garante e sviluppare strumenti tecnici e organizzativi che possano garantire lo svolgimento delle attività in coerenza con le disposizioni normative.
In tale contesto anche la diffusione agli operatori aziendali di adeguate norme di comportamento e di corrette regole per l'utilizzo della strumentazione elettronica nel rispetto dei principi fondanti della normativa privacy, risulta fondamentale in considerazione del fatto che l'attività sanitaria, per sua natura, "tratta dati" nell'accezione più ampia del termine e, nello specifico, "categorie particolari di dati personali" come meglio identificati nell'art. 9 del GDPR.

Art. 1 - Oggetto e scopo

Il presente Regolamento contiene disposizioni attuative del D.lgs. 196/03 e s.m.i. (Codice Privacy) e del Regolamento UE 2016/679 (GDPR) nell'ambito delle strutture dell'Azienda Usl della Romagna con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Azienda medesima. L'Azienda adotta idonee e preventive misure di sicurezza, volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. L'Azienda adotta, altresì, le misure occorrenti per facilitare l'esercizio dei diritti dell'interessato ai sensi degli artt. 15 e seg, del GDPR.

Art. 2 - Responsabilità e organizzazione

Le presenti linee guida si applicano a tutti i trattamenti di dati personali effettuati dall'Azienda U.S.L. della Romagna nello svolgimento delle proprie funzioni istituzionali. La responsabilità della corretta applicazione delle linee guida è attribuita al Titolare, ai Responsabili ed al personale "autorizzato" del trattamento dei dati personali, ciascuno in relazione all'ambito di rispettiva competenza. Si rinvia in merito ai successivi artt. 8 – 9 – 10 - 11.

L'Azienda USL della Romagna con delibera n. 510 del 10.11.2017 ha istituito il **Comitato Aziendale per la protezione dei dati personali**, quale organismo multidisciplinare preposto alla sicurezza nel suo complesso dei dati sotto l'aspetto clinico, organizzativo e di protezione dei dati trattati in Azienda, al fine di dare applicazione agli adempimenti previsti dal Regolamento UE n. 2016/679. Con successiva deliberazione n. 394 del 9.12.2019 il citato Comitato è stato rivisto nella sua composizione e allo stesso sono stati assegnati i seguenti specifici compiti:

- redigere il Manuale di aderenza al GDPR;
- redigere il documento "Livello di adozione del codice di condotta" che specifica le prescrizioni adottate dal titolare e previste dall'eventuale, futuro codice di condotta per la protezione dei dati personali per la sanità;
- aggiornare il Registro delle attività di trattamento dei dati;
- organizzare il Registro dei sistemi informatizzati compresi i dispositivi medici utilizzati nell'ambito dei trattamenti, definendone la struttura che dovrà essere redatto e aggiornato dall'UO GSI competente;
- aggiornare il Registro delle violazioni che ricomprende gli incidenti di sicurezza informatici aggiornati direttamente dall'UO GSI competente;
- assistere il titolare nel formalizzare e promuovere le procedure organizzative e la formazione in merito all'esecuzione dei vari trattamenti, sia relativamente alle attività informatizzate che a quelle manuali, nonché promuovere la sensibilizzazione della cultura sulla corretta applicazione della normativa privacy, anche coordinando le attività formative dei dipendenti in materia di tutela dei dati personali;

- contribuire alla formalizzazione e alla promozione di tutti documenti che il Titolare ritiene necessari per assicurare l'efficace pianificazione, funzionamento e tenuta sotto controllo del sistema;
- validare le procedure organizzative e le soluzioni tecnologiche implementate presso l'organizzazione relativamente agli aspetti di protezione dei dati personali e dei rischi connessi;
- fornire il necessario supporto alle varie strutture aziendali su temi multidisciplinari in ordine alle problematiche legate al trattamento dei dati, assicurando una visione complessiva che tenga conto delle esigenze dell'organizzazione;
- valutare periodicamente le caratteristiche del "Sistema di gestione per la protezione dei dati" e proporre alla Direzione i piani evolutivi necessari per assicurarne la continua efficacia ed idoneità rispetto alle esigenze dell'organizzazione;
- supportare il DPO per l'espletamento dei compiti ad esso affidati dalla normativa;
- svolgere azioni di monitoraggio periodico sull'accesso ai dati personali da parte del personale aziendale con particolare riguardo ai dati riservati sul DSE con il supporto dell'U.O. GSI;
- valutare/effettuare, con il supporto dell'U.O. GSI, la Valutazione d'impatto sulla protezione dei dati se necessario, ogniqualvolta si implementino nuovi trattamenti ed ogniqualvolta vengano attivate nuove attività e/o variate le tecnologie e le procedure nell'ambito di trattamenti e/o attività già in essere basate su dati non anonimi e non pseudonimizzati, con particolare riferimento alle attività finalizzate all'erogazione di servizi sanitari all'interessato
- definire la programmazione annuale di audit interno dell'Azienda;
- analizzare i risultati degli audit interni definendo le eventuali azioni correttive necessarie da porre in essere.
Per le funzioni del Comitato di norma viene invitato agli incontri il DPO aziendale.

Con la medesima deliberazione sono state, altresì, specificate le aree di responsabilità dell'U.O. Affari Generali e Direzione Percorsi Istituzionali e Legali e dell'U.O. Gestione sistemi Informative relativamente all'applicazione della normativa sul trattamento dei dati, nel rispetto di quanto previsto in merito nel Manuale dell'Assetto organizzativo di cui alla deliberazione n. 524/2015 per le citate U.O., come segue:

U.O. AFFARI GENERALI:
- assicurare il supporto alle articolazioni organizzative aziendali relativamente all'approfondimento normativo sulle problematiche legate al trattamento dei dati personali;
- svolgere attività di primo contatto/punto di riferimento con gli operatori interni ed esterni che necessitino di chiarimenti o approfondimenti sulle tematiche giuridiche in materia di privacy anche attraverso regolamenti e/o note esplicative per il corretto espletamento delle relative attività, fermo restando che le problematiche più complesse o di valenza strategico aziendale verranno trattate in seno al Comitato;
- garantire la formazione interna in materia mediante l'organizzazione e docenza di periodici corsi di aggiornamento rivolti a tutto il personale (amministrativo e sanitario);
- predisporre e aggiornare moduli di informativa per i pazienti/utenti da trasmettere ai Responsabili interni per l'affissione e supportare questi ultimi nella predisposizione di specifiche istruzioni per il trattamento dei dati agli operatori;

- pubblicare gli elenchi aggiornati dei responsabili interni del trattamento dei dati nel sito web aziendale con la collaborazione della U.O. Gestione giuridica risorse umane nonché aggiornare gli spazi di intranet ed internet dedicati alle informazioni sulla privacy;
- curare le pratiche di riscontro agli interessati per l'esercizio dei diritti previsti dalle normative in materia di trattamento dei dati personali;
- garantire gli aggiornamenti della normativa in materia anche attraverso la predisposizione/trasmissione linee guida;
- partecipare ai lavori della Commissione di videosorveglianza per valutazioni ad essa affidate dalla delibera istitutiva n. 568/2016 e s.m.i.

U.O. GESTIONE DEI SISTEMI INFORMATIVI

-collaborare con il DPO nell'esercizio delle sue funzioni attribuite dalla normativa, comprese le specifiche verifiche richieste dallo stesso;
- supportare il Comitato per la protezione dei dati personali nella valutazione/effettuazione della valutazione d'impatto;
- sovraintendere sulle attribuzioni di Amministratore di Sistema e tenere l'elenco aggiornato dei medesimi;
- garantire le misure di sicurezza poste a protezione dei dati trattati in modo informatizzato;
- adottare i regolamenti per l'utilizzo dei sistemi informativi e diffondere le corrette modalità di utilizzo degli strumenti informatici al personale anche attraverso l'organizzazione di corsi di formazione rivolti a tutto il personale;
- individuare le misure più adeguate ed efficienti per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Azienda;
- garantire l'evasione delle richieste di oscuramento dei dati secondo la normativa del Dossier sanitario elettronico (DSE) nonché di eventuali ulteriori richieste riguardanti i diritti degli interessati per la parte di competenza, riscontrando, nei tempi previsti dalla normativa vigente, all'U.O. Affari generali e direzione percorsi istituzionali e legali;
-tenere il Registro dei profili di abilitazione descrittivo dei profili definiti nei singoli sistemi informatizzati con l'individuazione dei relativi privilegi e delle persone fisiche afferenti ai profili stessi e dei relativi periodi di abilitazione, mantenendo la storia delle abilitazioni precedenti;
- effettuare verifiche periodiche delle abilitazioni degli utenti secondo i criteri previsti dalle disposizioni in materia di sicurezza dei sistemi informatici;
- gestire centralmente l'anagrafica degli utenti abilitati ai sistemi informatici contenente, oltre ai dati identificativi dell'utente stesso, le informazioni relative all'affiliazione dell'utente (dipendente/libero professionista ecc.), il periodo di abilitazione;
- redigere il Registro dei Sistemi informatizzati;
- tenere e aggiornare il Registro degli incidenti di sicurezza informatici;

Il **Data Protection Officer** (DPO), nominato dall'Azienda USL della Romagna ai sensi del Regolamento europeo 2016/679 con delibera n. 387 del 3.12.2019, svolge le funzioni previste dal GDPR e le ulteriori attività specificate nel contratto individuale di lavoro.

Art. 3 - Dati Personali -

Costituisce dato personale (art. 4 comma 1 del GDPR) qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato) anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. I dati sensibili, ora "dati di categoria particolare" ai sensi dell'art. 9 del GDPR, sono quei dati personali idonei a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, o i dati genetici o biometrici intesi a identificare in modo univoco una persona fisica nonché i dati relativi alla salute, o alla vita sessuale dell'interessato o all'orientamento sessuale della persona.

Art. 4 - Trattamento dei dati personali -

Con l'espressione "trattamento", ai sensi dell'art. 4, punto 2 del GDPR, deve intendersi qualunque operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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

In base a quanto prevede l'art. 2 sexies del D.lgs. 196/03 con le modifiche introdotte dal D.Lgs. 101/2018, i trattamenti delle categorie particolari di dati personali di cui all'art. 9 paragrafo 1 del GDPR, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2 lettera g) del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Ai sensi del comma 2 dell'art. 2 sexies, sopracitato, si considera rilevante l'interesse pubblico relativo ai trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di poteri pubblici nelle materie tassativamente elencate nel predetto articolo di legge.

In ottemperanza ai principi di necessità, pertinenza e non eccedenza dei dati, la pubblicazione dei provvedimenti aziendali contenenti dati sensibili avviene previa selezione dei soli dati la cui inclusione nelle deliberazioni medesime sia realmente necessaria per il raggiungimento delle finalità proprie di ciascun provvedimento. I soggetti cui si riferiscono le informazioni di carattere sensibile devono essere individuati attraverso l'utilizzo di codici alfanumerici; ogni dato di natura sensibile o giudiziaria (o appartenente a categorie particolari di dati personali ai sensi dell'art. 9 del GDPR), che possa essere isolato dal contesto del provvedimento, senza comprometterne la necessaria motivazione, è riportato in allegati non oggetto di pubblicazione o con il riferimento di protocollo.

Art. 5 - Criteri per l'esecuzione del trattamento dei dati personali -

Ogni trattamento di dati deve essere effettuato con modalità atte ad assicurare il rispetto dei diritti e della dignità dell'interessato. Oggetto di ogni tipo di trattamento dovranno essere i soli dati essenziali per lo svolgimento delle attività istituzionali. I dati personali devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in operazioni del trattamento in termini compatibili con tali scopi. I dati devono essere esatti, aggiornati, pertinenti e non eccedenti rispetto alle finalità per i quali sono raccolti e trattati.
E' compito dei Responsabili di trattamento verificare periodicamente la liceità e la correttezza dei trattamenti, l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisca di propria iniziativa. I dati che, anche a seguito di verifiche, risultassero eccedenti, non pertinenti o non indispensabili, non potranno essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto che li contiene.
In ogni caso devono essere adottate misure tecniche tali da garantire che i dati personali o sensibili siano accessibili al solo personale autorizzato al trattamento e nella misura strettamente indispensabile allo svolgimento delle mansioni di ciascuno.

Art. 6 - Consenso al trattamento dei dati -

A seguito dell'entrata in vigore del Regolamento UE n. 679/2016 ed in particolare con riferimento all'art. 9 comma 2 lett. h) e lett. i) e del comma 3 del medesimo Regolamento, l'Azienda USL della Romagna tratta i dati sanitari per finalità di prevenzione, diagnosi e cura, assistenza, terapia sanitaria o sociale, riabilitazione senza necessità del consenso dell'interessato.

Ulteriori particolari trattamenti di dati relativi alla salute saranno effettuati mettendo a disposizione dell'interessato informazioni integrative e richiedendo, se previsto, uno specifico ed esplicito consenso. Si tratta a titolo esemplificativo di trattamenti connessi:

- all'implementazione del Dossier Sanitario Elettronico o del Fascicolo Sanitario Elettronico;
- a scopi di ricerca scientifica anche nell'ambito delle sperimentazioni cliniche (tranne alcuni casi specifici previsti dalla legge);
- al trattamento dati genetici e/o biometrici;
- alla comunicazione di dati al medico o ad altri soggetti (es. Rete Sole)
- a servizi di refertazione on-line

Art. 7 - Comunicazione dei dati -

I dati relativi allo stato di salute non sono oggetto di diffusione (cioè non possono essere resi noti ad un numero indeterminato di soggetti); possono invece essere comunicati, nei casi previsti da norme di legge o di regolamento, a soggetti pubblici e privati, enti ed istituzioni per il raggiungimento delle rispettive finalità.

A titolo di esempio, si riportano alcuni soggetti cui l'Azienda può comunicare dati personali:

- soggetti pubblici (altre aziende sanitarie/enti sanitari) e privati (strutture sanitarie private, case di riposo), coinvolti nel percorso diagnostico-terapeutico del paziente;
- Ministero della Salute; Regione Emilia-Romagna o Regione di residenza (se diversa), per finalità amministrative di competenza regionale;
- Comune di residenza;
- Azienda sanitaria di residenza (se diversa da quella di accesso);
- Servizi Sociali dei Comuni per le attività connesse all'assistenza di soggetti deboli;
- Medici di Medicina Generale/Pediatri di Libera Scelta, quando previsto;
- soggetti qualificati ad intervenire in controversie in cui è parte l'Azienda (compagnie assicurative, legali e consulenti,ecc);
- Autorità Giudiziaria e/o Autorità di pubblica sicurezza, nei casi previsti dalla legge;
- Enti previdenziali per gli scopi connessi alla tutela della persona assistita;
- soggetti terzi che effettuino operazioni di trattamento dati personali per conto dell'Azienda, appositamente qualificati "responsabili esterni del trattamento" e tenuti al rispetto degli adempimenti in materia di protezione dati, in virtù di apposito contratto stipulato con l'Azienda;

Le persone ricoverate presso le strutture dell'Azienda o che accedono al Pronto Soccorso hanno il diritto, se espressamente richiesto, di comunicare le informazioni sullo stato di salute solo ai soggetti da essi individuati e di non rendere nota la propria presenza in reparto a soggetti terzi.

Art. 8 - Titolare del trattamento dei dati personali -

Il Titolare del trattamento, ai sensi dell'art. 4, punto 7 del GDPR, è l'Azienda USL della Romagna. Il Titolare, cui competono le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza, si avvale, in particolare anche se non in via esclusiva, per quanto attiene al principio di "responsabilizzazione" introdotto al punto 2 dell'art. 5 del GDPR, della figura del Responsabile del trattamento.

Art. 9 - Responsabili del trattamento dei dati personali -

In continuità con la precedente struttura organizzativa aziendale e nell'ottica del principio di responsabilizzazione introdotto al punto 2 dell'art. 5 del GDPR, con deliberazione n. 275 del 25/7/2018 sono stati individuati tutti i Direttori di struttura complessa, i Responsabili di struttura semplice dipartimentale, i Direttori di Distretti quali **Responsabili Interni del trattamento dei dati** (cosiddetti soggetti delegati), i cui compiti sono stati specificati con la medesima delibera.
I Responsabili interni del trattamento dei dati personali compiono tutto quanto è necessario per il rispetto delle vigenti disposizioni in tema di protezione dei dati (si richiama la deliberazione n. 275 del 25/7/2018 per i compiti ad essi assegnati); in particolare hanno il dovere di osservare e fare osservare le precauzioni individuate nel documento Linee guida per il trattamento e la tutela dei dati personali elaborato dall'Azienda. Ogni Responsabile interno del trattamento dei dati è nominato per iscritto dal Titolare del trattamento. La nomina viene notificata da parte dell'UO Gestione Giuridica Risorse Umane al momento dell'assunzione/ conferma degli incarichi di responsabilità predetti, unitamente ai compiti e istruzioni.

L'elenco completo dei Responsabili di Trattamento è pubblicato e aggiornato sul sito internet aziendale nonché sulla intranet, nelle sezioni privacy.

Art. 10 - Autorizzati del trattamento dati -

Chiunque tratti dati su istruzione del Titolare e del Responsabile è designato, per iscritto, quale **personale "autorizzato" di trattamento**, con riferimento all'art. 29 del GDPR mediante apposita modulistica. In particolare, come stabilito nella deliberazione n. 275/2018, sono identificati quali "autorizzati", i dipendenti e collaboratori, ed in generale tutti coloro che, pur in assenza di un rapporto di lavoro dipendente con l'Azienda, siano a vario titolo inseriti all'interno dell'organizzazione con svolgimento di operazioni di trattamento dei dati.
Ogni "autorizzato" al trattamento dei dati, a seconda della natura del rapporto in essere con l'Azienda USL della Romagna ha accesso ai soli dati la cui conoscenza sia strettamente necessaria al raggiungimento degli obiettivi propri del rapporto di lavoro. Gli autorizzati devono eseguire i trattamenti di dati secondo le disposizioni loro date dal Responsabile interno del trattamento, e nel rispetto di quanto previsto dalle presenti Linee guida e dal GDPR nonché di quanto previsto nelle Regolamento utilizzo dei sistemi informatici aziendali, pubblicato sul sito internet dell'azienda e sulla intranet . La nomina ad "autorizzato" decorre dalla decorrenza del rapporto di servizio.
Le istruzioni generali consegnate all'autorizzato sono integrate, come indicato nelle medesime istruzioni, dalle disposizioni contenute dal Regolamento per l'utilizzo dei sistemi informatici aziendali, reperibile sulla intranet aziendale, al quale si rinvia, per quanto attiene ai comportamenti da adottare per il corretto trattamento dei dati con modalità informatiche.
Ulteriori istruzioni specifiche potranno essere fornite dai Responsabili interni in materia di privacy ai propri collaboratori.

Art. 11 - Trattamento di dati affidati all'esterno

Agli Enti, organismi, soggetti pubblici e privati esterni all'Azienda, ai quali siano affidati attività o servizi o forniture di dispositivi che comportano il trattamento di dati personali per conto dell'Azienda USL, viene attribuita la qualità di **Responsabile Esterno del trattamento dei dati,** ai sensi dell'art. 28 del GDPR.
Le strutture aziendali competenti per la stipula e sottoscrizione dei contratti di cui sopra devono provvedere alla predisposizione e sottoscrizione dell'atto/contratto di nomina a Responsabile esterno del trattamento, tenendo conto che, il Regolamento Generale (UE) 2016/679 sulla protezione dei dati personali (di seguito anche GDPR o Regolamento), dispone che qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a responsabili del trattamento che garantiscano l'adozione di misure tecniche ed organizzative adeguate, in modo tale che il trattamento sia conforme alla normativa in materia di protezione dati e garantisca la tutela dei diritti dell'interessato.
Salvo che l'atto di nomina a Responsabile esterno non sia già inserito all'interno del contratto/ convenzione, le succitate strutture aziendali dovranno provvedere, di norma, alla nomina a Responsabile Esterno con atto separato. Sul sito intranet aziendale è rinvenibile lo schema tipo di riferimento adattabile alle specifiche esigenze.

Art. 12 - Informativa -

L'informativa è l'elemento necessario e fondamentale per la liceità di ogni forma di trattamento dei dati in quanto garantisce l'evidenza e la trasparenza delle attività specifiche che sono poste in essere.
L'informativa è sempre dovuta a prescindere dall'obbligo di acquisizione del consenso.

Essa deve contenere gli elementi tassativamente indicati dall'art. 13 del GDPR 2016/679 e più specificatamente:

- gli estremi identificativi del Titolare e del Responsabile della protezione dei dati e i dati utili per un contatto
- le finalità e le modalità con le quali vengono trattati i dati;
- l'obbligatorietà o meno del conferimento dei dati;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e ambito di diffusione dei dati medesimi;
- I tempi di conservazione dei dati
- i diritti dell'interessato, di cui all'articolo successivo;
- gli estremi identificativi del Titolare e del Responsabile della protezione dei dati e i dati utili per un contatto

La predetta informativa può essere resa anche tramite affissione di apposita cartellonistica nei locali di accesso all'utenza.

L'Azienda USL della Romagna ha inserito la propria informativa generale, unitamente all'informativa sul Dossier Sanitario anche nel proprio sito internet, nella sezione privacy dedicata.

Nelle more della approvazione del documento aziendale sul Dossier Sanitario elettronico (DSE) che conterrà le specifiche applicative per il corretto utilizzo di tale strumento informatico all'interno della Ausl Romagna in conformità alle indicazioni di cui alle Linee Guida Garante Privacy del 04.06.2015 richiamate nel Provvedimento del Garante n. 55 del 7.3.2019, si rinvia a quanto già disciplinato nelle precedenti Linee Guida Privacy adottate con deliberazione n. 600/2017 per quanto attiene gli aspetti applicativi del Dossier sanitario.

Art. 13 - Diritti dell'interessato

I diritti degli interessati sono disciplinati agli articoli da 15 a 22 del Regolamento UE 2016/679 e sono elencati qui di seguenti:

- Diritto alla trasparenza del titolare del trattamento, diritto all'accesso
- Diritto di rettifica
- Diritto alla cancellazione dei dati
- Diritto alla limitazione del trattamento
- Diritto alla portabilità del trattamento

- Diritto di opposizione al trattamento
- Diritti relativi alla decisione automatizzata e alla profilazione

In particolare:

- il **diritto alla rettifica** (art. 16 del GDPR) può essere attivato in presenza di dati inesatti o incompleti
- il **diritto alla cancellazione** (art. 17 del GDPR) consiste nella facoltà di ottenere dal Titolare la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nel rispetto delle condizioni del GDPR. Le strutture sanitarie pubbliche sono esentate dall'applicazione del diritto alla cancellazione sul trattamento dei dati effettuati in quanto, come stabilito dal paragrafo 3 lett. c) dell'art. 17 del GDPR trattano dati di interesse pubblico nel settore della sanità pubblica in conformità dell'art. 9 paragrafo 2 , lettera h) e i) e dell'art. 9 , paragrafo 3;
- il **diritto alla limitazione** (art. 18 del GDPR) consiste nella possibilità di opporsi al trattamento dei propri dati personali, da specificare nella richiesta, oppure senza necessità di motivare l'opposizione quando i propri dati sono trattati per finalità di marketing diretto . E' esercitabile non solo in caso di mancanza dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l´interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento ai sensi dell´art. 21 del Regolamento (in attesa della valutazione da parte del titolare
- il **diritto alla Portabilità** (art. 20) è uno dei nuovi diritti previsti dal regolamento europeo .Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono "portabili" solo i dati trattati con il consenso dell´interessato o sulla base di un contratto stipulato con l´interessato (quindi non si applica ai dati il cui trattamento si fonda sull´interesse pubblico, o sull´interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"**forniti" dall´interessato al titolare *(si veda il considerando 68 per maggiori dettagli)*.
  Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall´interessato, se tecnicamente possibile.
- Il **diritto all'opposizione** (art. 21 GDPR) Il diritto di opposizione è applicabile alle strutture sanitarie pubbliche: pur essendo il trattamento effettuato da quest'ultime necessario per l'esecuzione di un compito svolto nel pubblico interesse (art. 6.1 lett e) del GDPR), all'interessato deve essere in ogni caso riconosciuto il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. Al riguardo incombe sulla struttura sanitaria pubblica che ritenga di non ottemperare alla richiesta di opposizione, di dimostrare che i suoi interessi legittimi cogenti prevalgono sui diritti e sulle liberta fondamentali dell'interessato (considerando 69 GDPR)
- i **diritti relativi alla decisione automatizzata e alla profilazione** (art. 22 GDPR). L'interessato ha diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona

L'interessato che ritenga che il trattamento dei dati personali che lo riguardi sia stato effettuato in violazione di legge, ha il diritto di proporre un reclamo all' Autorità Garante per la protezione dei dati personali ovvero all'autorità di controllo dello stato membro UE in cui risiede abitualmente , lavora ovvero del luogo ove si è verificata la presunta violazione secondo le procedure previste dall'art. 77 del GDPR.

Modalità per l'esercizio dei diritti:
L'interessato potrà esercitare i Suoi diritti presentando istanza all'Azienda Usl della Romagna, titolare del trattamento dei dati, possibilmente utilizzando l''apposito modulo scaricabile dal sito internet aziendale.

L'istanza può essere, altresì, inviata al Responsabile della protezione dei dati al seguente indirizzo e-mail : dpo@auslromagna.it o per posta ordinaria all'indirizzo Azienda Usl della Romagna, via De Gasperi n. 8 – 48121 Ravenna (alla c.a. UO Affari generali e percorsi istituzionali e legali).

Termine:
Il termine per la risposta all´interessato è, per tutti i diritti (compreso il diritto di accesso), di 1 mese**,** estendibili fino a 3 mesi in casi di particolare complessità**;** il titolare deve comunque dare un riscontro all´interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Spetta al Titolare valutare la complessità del riscontro all´interessato e stabilire l´ammontare dell´eventuale contributo da chiedere all´interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art. 12 GDPR comma.5)*,* ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso *(*art. 15, paragrafo 3)*;* in quest´ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti.

Il riscontro all´interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l´accessibilità; può essere dato oralmente solo se così richiede l´interessato stesso *(*art. 12, paragrafo 1e art. 15, paragrafo 3del GDPR).

Art. 14 - Il Registro delle attività di trattamento

L'Azienda dispone, come stabilito dall'art. 30 del GDPR, di un Registro delle attività di trattamento predisposto secondo le indicazioni regionali.
Il Registro contiene la rilevazione delle attività di trattamento suddivise per tipologia e contiene le informazioni previste dal citato art. 30. Come previsto dalla deliberazione n. 394 del 9/12/2019 è aggiornato dal Comitato aziendale per la Protezione dei dati.

Art. 15 - Rinvio a previsioni di normativa speciale

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali. In particolare:

a. dall'art. 5, comma 2, della Legge 5 giugno 1990, n. 135, come modificato dall'art. 178 del Codice, secondo cui la rilevazione statistica della infezione da HIV deve essere effettuata con modalità che non consentano l'identificazione della persona nonchè dalla prescrizione del Garante Privacy del 12.11.2009 in materia di raccolta dati sull'HIV a termini della quale l'esercente la professione sanitaria è tenuto a raccogliere un'anamnesi del paziente e ad illustrare a quest'ultimo l'importanza di tale raccolta di dati personali; l'interessato è comunque libero di scegliere in modo informato – e quindi consapevole – di non comunicare al medico alcune informazioni sanitarie richieste (cfr. Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario del 16.07.2009 par. n. 3), con particolare riferimento al diritto riconosciuto all'interessato di non comunicare ad un medico informazioni sanitarie che lo riguardano;
b. dall'art. 11 della Legge 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di cura o il poliambulatorio nei quali è effettuato un intervento di interruzione di gravidanza devono inviare alla Regione una dichiarazione che non faccia menzione dell'identità della donna;
c. dall'art. 734-bis del Codice Penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale;
d. dal D.P.R. 09.10.1990 n. 309 in materia di uso di sostanze psicotrope e di alcol.
Restano altresì fermi gli obblighi di legge che vietano la rivelazione, senza giusta causa, e l'impiego a proprio o altrui profitto delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti, in particolare, dal Codice di deontologia medica adottato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri.

Art. 16 - Altre misure per il rispetto dei diritti degli interessati

Ogni Responsabile del trattamento è tenuto a garantire, nell'ambito della propria articolazione organizzativa ed in relazione all'attività istituzionale di propria competenza, adeguate misure organizzative finalizzate a garantire il rispetto della dignità della persona e il massimo livello di tutela degli interessati in ambito sanitario.

Le misure di cui al comma precedente comprendono, in particolare:
a) l'adozione di soluzioni organizzative volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
b) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere. E' opportuno che vengano predisposte distanze di cortesia per operazioni amministrative allo sportello (prenotazioni) o al momento dell'acquisizione di informazioni sullo stato di salute, sensibilizzando anche gli utenti con cartelli, segnali ed inviti;
c) l'adozione di soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute e l'adozione di cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, si svolgano in situazioni di promiscuità derivanti dalle modalità o dai locali

prescelti. Quando prescrive medicine o rilascia certificati, il personale sanitario deve evitare che informazioni sulla salute dell'interessato possano essere conosciute da terzi. Lo stesso obbligo vale per la consegna di documentazione (analisi, cartelle cliniche, prescrizioni, ecc.), quando questa avvenga in situazioni di promiscuità (es. locali per più prestazioni, sportelli);

d) il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati. La tutela della dignità della persona deve essere sempre garantita, in particolare riguardo a fasce deboli (disabili, minori, anziani), ma anche a pazienti sottoposti a trattamenti medici invasivi o per i quali è doverosa una particolare attenzione (ad esempio, interruzione della gravidanza). Nei reparti di rianimazione devono essere adottati accorgimenti anche provvisori (es. paraventi) per delimitare la visibilità dell'interessato, durante l'orario di visita, ai soli familiari e conoscenti;
e) la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di Pronto Soccorso. L'organismo sanitario può dare notizia, anche per telefono, sul passaggio o sulla presenza di una persona al Pronto Soccorso, ma solo ai terzi legittimati, come parenti, familiari, conviventi. L'interessato, se cosciente e capace, deve essere preventivamente informato (es. all'accettazione) e poter decidere a quali soggetti può essere comunicata la sua presenza al pronto soccorso;
f) la formale previsione di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà. Le strutture sanitarie possono dare informazioni sulla presenza dei degenti nei reparti, ma solo a terzi legittimati (familiari, conoscenti, personale volontario). Anche qui l'interessato, se cosciente e capace, deve essere informato al momento del ricovero e poter decidere quali soggetti possono venire a conoscenza del ricovero e del reparto di degenza, compilando il modulo previsto al successivo art. 18 della presente Procedura;
g) la messa in atto di procedure dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute. Non è a tale proposito giustificata l'affissione di liste di pazienti in attesa di intervento in locali aperti al pubblico, con o senza la descrizione della patologia sofferta. Non devono inoltre essere resi visibili ad estranei documenti sulle condizioni cliniche dell'interessato, evitando, ad esempio, di porre le cartelle infermieristiche vicino al letto di degenza. Tali garanzie devono essere assicurate nelle eventuali certificazioni richieste per fini amministrativi non correlati a quelli di cura (ad esempio per giustificare un'assenza dal lavoro o l'impossibilità di presentarsi ad una procedura concorsuale).
h) la sottoposizione degli "autorizzati" che rivestono qualifiche professionali rispetto alle quali non è previsto per legge il segreto professionale, a regole di condotta analoghe al segreto professionale;
i) il rispetto di specifiche cautele in occasione di prestazioni sanitarie con le quali si perseguono anche finalità didattiche, oltre che di cura e prevenzione. In particolare, durante tali prestazioni devono essere adottate misure idonee a limitare l'eventuale disagio dei pazienti, anche in relazione al grado di invasività del trattamento, circoscrivendo, ad esempio, il numero degli studenti presenti e rispettando eventuali legittime volontà contrarie degli interessati;

j) I referti, sono consegnati in busta chiusa e possono essere ritirati dal diretto interessato o da chi esercita la tutela, in caso di minore o interdetto oppure dal delegato dell'interessato munito di delega, di fotocopia di un documento di identità del delegante e fotocopia del proprio documento di identità, salvo diverse disposizioni di legge o regolamento. La trasmissione dei referti tramite servizio postale è possibile soltanto con espressa richiesta preventiva da parte dell'interessato, rilasciata al momento della prestazione. La consegna dei referti è possibile anche On Line tramite Fascicolo Sanitario Elettronico, se attivato.

Art. 17 - Comunicazione di dati sanitari all'interessato

I dati personali idonei a rivelare lo stato di salute possono essere resi noti:

- all'interessato;
- ad un soggetto appositamente delegato per iscritto dall'interessato, mediante compilazione e sottoscrizione di apposito modulo.

In caso di impossibilità fisica, incapacità di agire o incapacità di intendere e di volere dell'interessato:

- a chi esercita legalmente la potestà;
- a un prossimo congiunto, a un familiare, a un convivente o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato.

Art. 18 - Responsabilità in caso di violazione delle disposizioni sulla privacy

Ai sensi dell'articolo 82 del Regolamento 2016/679: "Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento".

Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è punito con le sanzioni di natura amministrativa e di natura penale nelle ipotesi previste dagli articoli da 166 a 172 del Codice Privacy.
Inoltre si richiama quanto previsto dall'art. 615 ter c.p. nonché, sotto il profilo disciplinare si rinvia a quanto previsto dal CCNL 19/12/2019 dell'area Sanità per la dirigenza medica, veterinaria, sanitaria e dirigenza delle professioni sanitarie, dal CCNL 6/10/2010 per la dirigenza professionale, tecnica e amministrativa, dal CCNL 21/5/2018 per il personale del comparto sanità, nonché da quanto previsto dal DPR 62/2013 e dal Codice di Comportamento aziendale dell'AUSL della Romagna.

Art. 19 – Modulistica

L'Azienda USL della Romagna ha predisposto l'informativa per gli utenti che accedono alle strutture sanitarie e altre tipologie di utenti (es. i dipendenti) e la modulistica collegata alle presenti Linee guida.
Le informative e la modulistica aggiornate sono pubblicate nella Sezione Privacy del sito Internet e, altresì, nella Sezione Privacy sulla rete intranet aziendale.