

Luca Di Leo

*Consulenza e formazione in materia
di protezione dei dati personali dal 2005*

Studio Paci &C srl
(cda)

**Associazione Protezione diritti e
libertà privacy**
(Vice presidente)



Contatti:
info@lucadileo.it
Cell. 3931019939
www.consulenzepaci.it
Linkedin: #luca di leo

Responsabile della Protezione dei Dati (DPO per aziende private, pubbliche, sanità)
certificazione UNI 11697:2017 (Registro Accredia)

Valutatore Privacy
certificazione UNI 11697:2017 (Registro Accredia)

Privacy Officer
Certificazione TUV Italia 2013 – certificazione competenze Federprivacy – Legge n.4/2013

Auditor GDPR
secondo lo schema di certificazione per il GDPR: ISDP@10003 (Registro AICO SICEV)

**Consulente per l'implementazione dello schema di certificazione
ISDP@10003**
(Ente di certificazione INVEO)

Lead Auditor ISO 27001 , aggiornamento ISO 27701

PREMESSA

Il valore della protezione dei dati personali

La protezione dei dati quale riconoscimento di un diritto costituzionalmente garantito

Privacy non significa soltanto diritto di essere lasciati in pace o di proteggere la propria sfera privata

Diritto di controllare l'utilizzo e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione

La protezione dei dati personali è un diritto fondamentale perché tutela la dignità, la libertà, l'identità personale, l'eguaglianza, la non discriminazione, la riservatezza degli individui nei confronti dei soggetti pubblici e privati

**Il diritto alla protezione dei
dati personali non è solo un
diritto ma garanzia di libertà e
democrazia**

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Si rende ancora più necessaria l'adozione di politiche sulla sicurezza per tutelare i dati di chi si avvale della rete e dei servizi offerti da enti pubblici e privati

Vanno garantiti i canali di trasmissione e la connessione fra le banche dati.

Per raggiungere la compliance al GDPR è fondamentale la collaborazione fra professionisti e la creazione di modelli integrati

La protezione dei dati personali è
contemplata dall'articolo 8 della Carta
dei diritti dell'Unione Europea

Carta dei diritti dell'Unione Europea

Art. 8 - Protezione dei dati di carattere personale

1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Considerando 4 Regolamento Europeo 2016/679

(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.

Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

Ricordiamo che per «dato personale» si intende:

Qualsiasi informazione (iniziali del nome, cognome, qualsiasi numero o codice di riferimento associabile al soggetto, numero di ordine, codice fiscale, firma, fotografia, etc.) riconducibile direttamente o indirettamente anche attraverso il confronto con altre banche dati, ad una persona fisica.

I DATI PSEUDOANONIMIZZATI E/O CIFRATI SONO ANCORA DATI PERSONALI.

LA PSEUDOANONIMIZZAZIONE E LA CIFRATURA SONO MISURE DI SICUREZZA E NON UNA TIPOLOGIA DI DATI PERSONALI

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Art. 4 - Dato personale: qualsiasi informazione riguardante una 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

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

A titolo esemplificativo si considerano dati personali:

Il nome ed il cognome, il numero di telefono o di cellulare ovvero l'indirizzo e – mail, i dati della carta di credito, i dati relativi ad un pagamento, la rilevazione della temperatura, il codice fiscale, l'immagine fotografica di una persona, le riprese video, una registrazione vocale, una targa automobilistica, un indirizzo IP, la cronologia della navigazione web, impronta digitale, la scansione della retina, le coordinate GPS, le analisi cliniche (pressione sanguigna, il livello di diabete ecc)

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Art. 9 - Categorie particolari di dati personali:

Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

SPECIFICA SUI DATI RELATIVI ALLA SALUTE:

- Dati personali attinenti alla salute fisica o mentale di una persona fisica;
- La prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative allo stato di salute;
- Il semplice fatto di avere prenotato una prestazione di servizi di assistenza sanitaria da parte dei soggetti interessati;
- Prescrizioni di farmaci anche se codificati, ricette «bianche», relazioni mediche o fisioterapiche, certificati o stato di disabilità, ausilio di presidi medici quali carrozzine, stampelle, pannoloni, etc.
- Un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari (es. numero della coda per un servizio specialistico);
- Le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; (esami del sangue, urine, diagnostica, reperti e referti, lastre, etc)
- Qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici;
- Lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro;

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Art. 10 - Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza è consentito solo sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

Si tratta dei dati c.d. *"giudiziari"*, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Articolo 4 - 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

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Operazioni di trattamento dati

- | | |
|--|--|
| <ul style="list-style-type: none">- raccolta,- la registrazione,- l'organizzazione,- la strutturazione,- la conservazione,- l'adattamento o- la modifica,- l'estrazione,- la consultazione, | <ul style="list-style-type: none">- 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; |
|--|--|

Articolo 9

Trattamento di categorie particolari di dati personali

1. È 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.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) consenso, b) lavoro: diritto del lavoro, sicurezza e protezione sociale, contratto collettivo, etc. c) interessi vitali d) associazioni, e) dati resi manifestatamente pubblici dall'interessato f) difendere un diritto in sede giudiziaria g) motivi di interesse pubblico rilevante (**art. 2 sexies D.Lgs. 196/2003**) h) diagnosi assistenza e terapia sanitaria, medicina preventiva e del lavoro – trattamenti effettuati da professionisti sanitari sulla base del diritto UE o dello stato membro i) interesse pubblico settore sanità (minacce gravi sulla salute) j) archiviazione pubblico interesse, ricerca scientifica, storica, statistica

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di

segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (C53)

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Art. 2-sexies

(Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante).

Art. 2-septies

((Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute).))

5) Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalita' del trattamento e possono individuare, in conformita' a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati e' consentito.

In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalita' per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonche' le eventuali altre misure necessarie a garantire i diritti degli interessati.

Provvedimento che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2016 che risultano compatibili con il Regolamento e con il d.lgs. n. 101/2018 di adeguamento del Codice - 13 dicembre 2018 [9068972]

1. Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. gen. n. 1/2016);
2. Prescrizioni relative al trattamento di categorie particolari di dati da parte degli organismi di tipo associativo, delle fondazioni, delle chiese e associazioni o comunità religiose (aut. gen. n. 3/2016);
3. Prescrizioni relative al trattamento di categorie particolari di dati da parte degli investigatori privati (aut. gen. n. 6/2016);
4. Prescrizioni relative al trattamento dei dati genetici (aut. gen. n. 8/2016);
5. Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica (aut. gen. n. 9/2016).

Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario - 7 marzo 2019 [9091942]

Il trattamento dei dati sulla salute è consentito in presenza di taluni requisiti specifici individuati all'art. 9 del Regolamento (cfr. considerando n. 51), il quale ha previsto, in questo ambito, la possibilità per gli Stati membri di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riferimento al predetto trattamento (cfr. art. 9, par. 4). Il decreto legislativo n. 101/2018, in vigore dal 19 settembre 2018, ha previsto, al riguardo, che il Garante completi l'individuazione dei presupposti di liceità dei suddetti trattamenti, adottando specifiche misure di garanzia e promuovendo l'adozione di regole deontologiche (artt. 2-septies e 2-quater del Codice).

Le deroghe al divieto generale di trattare le cc.dd. "categorie particolari di dati", tra cui rientrano quelli sulla salute, sulla base delle quali è ammesso il trattamento di tali dati, sono ora da individuarsi nell'art. 9 del Regolamento che elenca una serie di eccezioni che rendono lecito il trattamento e che, in ambito sanitario, sono riconducibili, in via generale, ai trattamenti necessari per:

- a. **motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri** (art. 9, par. 2, lett. g) del Regolamento), individuati dall'art. 2-sexies del Codice;
- b. **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 preveda misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (art. 9, par. 2, lett. i) del Regolamento e considerando n. 54) (es. emergenze sanitarie conseguenti a sismi e sicurezza alimentare);
- c. **finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali** (di seguito "finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, (art. 9, par. 2, lett. h) e par. 3 del Regolamento e considerando n. 53; art. 75 del Codice) 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.

Con riferimento ai trattamenti in ambito sanitario che non rientrano nelle ipotesi sopra descritte e, quindi, che richiedono il consenso esplicito dell'interessato (art. 9, par. 2, lett. a) del Regolamento), si individuano, a titolo esemplificativo, le seguenti categorie:

- a. trattamenti connessi all'utilizzo di App mediche, attraverso le quali autonomi titolari raccolgono dati, anche sanitari dell'interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato possano avere accesso soggetti diversi dai professionisti sanitari o altri soggetti tenuti al segreto professionale (cfr. Faq CNIL del 17 agosto 2018 sulle applicazioni mobili in sanità⁽¹⁾);
- b. trattamenti preordinati alla fidelizzazione della clientela, effettuati dalle farmacie attraverso programmi di accumulo punti, al fine di fruire di servizi o prestazioni accessorie, attinenti al settore farmaceutico-sanitario, aggiuntivi rispetto alle attività di assistenza farmaceutica tradizionalmente svolta dalle farmacie territoriali pubbliche e private nell'ambito del Servizio sanitario nazionale (SSN);
- c. trattamenti effettuati in campo sanitario da persone giuridiche private per finalità promozionali o commerciali (es. promozioni su programmi di screening, contratto di fornitura di servizi amministrativi, come quelli alberghieri di degenza);
- d. trattamenti effettuati da professionisti sanitari per finalità commerciali o elettorali (cfr. provv. del 6 marzo 2014, doc. web n. 3013267);
- e. trattamenti effettuati attraverso il Fascicolo sanitario elettronico (d.l. 18 ottobre 2012, n. 179, art. 12, comma 5) In tali casi, l'acquisizione del consenso, quale condizione di liceità del trattamento, è richiesta dalle disposizioni di settore, precedenti all'applicazione del Regolamento, il cui rispetto è ora espressamente previsto dall'art. 75 del Codice. Al riguardo, un'eventuale opera di rimeditazione normativa in ordine all'eliminazione della necessità di acquisire il consenso dell'interessato all'alimentazione del Fascicolo, potrebbe essere ammissibile alla luce del nuovo quadro giuridico in materia di protezione dei dati.

Estratto dal Provv. 9 novembre 2005 Garante per la Protezione dei dati personali

Comunicazione dello stato di salute all'interessato

Gli esercenti le professioni sanitarie possono comunicare all'interessato informazioni sul suo stato di salute **solo per il tramite di un medico.**

(individuato dallo stesso interessato, oppure dal titolare del trattamento) o di un altro esercente le professioni sanitarie che, nello svolgimento dei propri compiti, intrattenga rapporti diretti con il paziente (ad es., un infermiere designato quale incaricato del trattamento ed autorizzato per iscritto dal titolare).

Nel caso in cui l'interessato riceva una comunicazione che documenti gli esiti di esami clinici effettuati, l'intermediazione può essere soddisfatta accompagnando un giudizio scritto con la disponibilità del medico a fornire ulteriori indicazioni a richiesta.

Il personale designato deve essere istruito debitamente anche in ordine alle modalità di consegna a terzi dei documenti contenenti dati idonei a rivelare lo stato di salute dell'interessato (es. referti diagnostici).

MISURE DI SICUREZZA

Estratto dal Provv. 9 novembre 2005 Garante per la Protezione dei dati personali

Formazione specifica per gli operatori sanitari e operatori autorizzati a trattare dati sanitari

La formazione deve essere specifica in merito ai trattamenti dati sulla salute, alla comunicazione, alla divulgazione ed i rischi connessi a tali trattamenti dati.

Riservatezza nei colloqui e nelle prestazioni

É doveroso adottare idonee cautele in relazione allo svolgimento di colloqui, specie fra il personale sanitario (ad es. in occasione di gestione delle prescrizioni o presentazione di certificazioni mediche), per evitare che in tali occasioni le informazioni sulla salute dell'interessato possano essere conosciute da terzi.

ART. 83 D.LGS. 196/2003 – ABROGATO DAL D.LGS. 101/2018

RICHIAMATO NEL PROV. DEL 2005 «RISPETTO DELLA DIGNITA'»

ATTUALMENTE APPLICABILE COME «MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE»

1. I soggetti di cui agli articoli 78, 79 e 80 adottano idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.

ART. 83 D.LGS. 196/2003 – ABROGATO DAL D.LGS. 101/2018 ma attuale e

ripreso nel provvedimento sul «rispetto della dignità»

2. Le misure di cui al comma 1 comprendono, in particolare:

1.a) soluzioni 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;

1.b) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;

1.c) soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;

1.d) cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

1.e) il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;

1.f) 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;

1.g) la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, 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;

1.h) la messa in atto di procedure, anche di **formazione del personale**, 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;

1.i) la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

2-bis. Le misure di cui al comma 2 non si applicano ai soggetti di cui all'articolo 78, che ottemperano alle disposizioni di cui al comma 1 secondo modalità adeguate a garantire un rapporto personale e fiduciario con gli assistiti, nel rispetto del codice di deontologia sottoscritto ai sensi dell'articolo 12.]

Misure tecniche/organizzative raccomandate per mitigare il rischio

idonee cautele quali:

- **distanze di sicurezza,**
- **barriere fisiche (es. bandelle),**
- **barriere visive (es. segnaletica colorata a terra, cartelli riportanti avvisi per mantenere la distanza di sicurezza),**
- **parlare a bassa voce,**
- **eventualmente isolare il paziente per comunicazioni particolari,**
- **fare uscire le altre persone dalla stanza (o dalle aree) che non sono legittimate alla ricezione di informazioni del paziente, in relazione allo svolgimento di colloqui, specie con il personale sanitario (ad es. in occasione di prescrizioni o di certificazioni mediche, o nella raccolta di informazioni o documenti in fase di anamnesi**
- **FORMAZIONE / ISTRUZIONI – anche la formazione e le istruzioni sono una misura di sicurezza!!!**

Il dato sanitario, fonte e risultato di analisi e valutazioni cliniche, è un valore fondamentale che deve essere non solo utilizzato per assicurare le migliori cure all'interessato, ma anche preservato e trattato nel rispetto della dignità dell'individuo e dei principi fondamentali del Regolamento europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, che richiede che il trattamento delle informazioni sia al servizio dell'uomo, dovendo considerare il diritto alla protezione dei dati alla luce della sua funzione sociale (Considerando n. 4 del Regolamento UE 2016/679).

In tale contesto, è necessario evidenziare che lo stesso ordinamento appresta specifiche tutele con riferimento a particolari tipologie di interventi sanitari o di patologie caratterizzate da una forte stigmatizzazione sociale in cui la dignità dei pazienti, soggetti per loro natura vulnerabili, è ancor più esposta. In molti provvedimenti, anche recenti e purtroppo talvolta di natura sanzionatoria, l'Autorità ha ricordato la necessità che l'erogazione delle prestazioni sanitarie, anche in emergenza, sia effettuata nel pieno rispetto soprattutto delle fasce più deboli quali i disabili, fisici e psichici, i minori, gli anziani e i soggetti che versano in condizioni di disagio o bisogno, garantendo altresì le specifiche tutele previste a favore delle vittime di violenza, di chi chiede l'accesso a percorsi clinici in anonimato e dei pazienti affetti da HIV.

Le condizioni con cui operano i professionisti sanitari, specie nei pronto soccorso, caratterizzate dalla mancanza di spazi adeguati e di risorse organizzative e umane, non può costituire un ostacolo al pieno rispetto dei diritti fondamentali dell'individuo specie in un contesto come quello sanitario in cui le fragilità sono più evidenti.

Si richiamano pertanto codesti Enti a:

garantire il pieno rispetto dei diritti fondamentali dell'individuo connessi al trattamento dei dati sanitari,

a proseguire l'opera di formazione degli operatori sanitari prevista dal Regolamento e a

vigilare affinché, nell'erogazione dei servizi sanitari, anche attraverso le nuove modalità offerte dalla sanità digitale, la protezione dei dati personali sia considerata un valore fondante sin dalla progettazione degli stessi.

PRINCIPI E DEFINIZIONI

Accountability

Articolo 5 Reg. UE 2016/679

Principi applicabili al trattamento di dati personali

1. I dati personali sono: (C39)

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»). (C74)

Accountability

Articolo 24 Reg. UE 2016/679

Responsabilità del titolare del trattamento (C74-C78)

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Accountability

Principi applicabili al trattamento dei dati personali

Liceità e trasparenza

Finalità

Minimizzazione

Esattezza

Limitazione della Conservazione

Misure di sicurezza

Revisione periodica o all'occorrenza delle politiche (art. 24 GDPR)

Accountability

Principi applicabili al trattamento dei dati personali

Trasparenza: **Informazioni sul trattamento dei dati (art. 13 GDPR)**

"misure appropriate" (art. 12, par. 1, del Regolamento).

- Titolare è responsabile per:

decidere le modalità e il formato più adeguati per fornire all'interessato le indicazioni richieste dall'informativa, tenere conto del contesto, circostanze, es. cartaceo, telefonico, Web, APP, Tablet, tecnologie intelligenti, interazioni con ambiente fisico. L'interfaccia web a disposizione

- Informazioni troppo dettagliate e difficilmente comprensibili,
- Rendere l'informativa su più livelli in modo da consentire agli interessati di acquisire i necessari approfondimenti in fasi successive o di consultare particolari aspetti dell'informativa che giudicano di maggiore interesse
- informazioni possono essere fornite "in combinazione" con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile
- no a soli link

Principi applicabili al trattamento dei dati personali

Liceità – basi giuridiche

- consenso (APP mediche, fidelizzazione della clientela, marketing, FSE (non più), Dossier Sanitario (SI))
- qualora l'interessato si trovi nell'incapacità fisica o giuridica per tutelare un interesse vitale
- manifestamente pubblici dall'interessato
- interesse pubblico rilevante e (art. 2 sexies - D.Lgs. 196/2003)
- medicina del lavoro, diagnosi, assistenza o terapia o sociale, gestione servizi sanitari o sociali, sulla base dei diritto dell'Unione
- motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute. ...
- archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

Accountability

Principi applicabili al trattamento dei dati personali

Finalità:

- Prenotazione on line di prestazioni sanitarie, attività di prevenzione, diagnosi, cura e riabilitazione, (finalità di cura) servizi diagnostici, programmi terapeutici e qualsiasi altro servizio sanitario erogato nell'ambito dell'assistenza specialistica e ambulatoriale, della diagnostica e di ricovero, fornitura di beni o servizi all'utente attraverso una rete di comunicazione elettronica, attività organizzative, amministrative, e di gestione dei servizi forniti agli utenti, riguardanti l'attività di prenotazione, di pagamento e di accettazione, fatturazione delle prestazioni, attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria. Rendicontazione e trasmissione elettronica dei dati sulla base della normativa vigente agli enti istituzionali competenti, trasmissione al sistema Tessera TS salvo diniego dell'utente, alimentazione del FSE – Fascicolo Sanitario Regionale secondo le disposizioni del Decreto Legge 18 ottobre 2012, n. 179, convertito, con modificazioni dalla Legge 17 dicembre 2012,
- Referti on line - DPCM dell'8 agosto 2013
- Attività di marketing

Accountability

Principi applicabili al trattamento dei dati personali

Minimizzazione:

- Individuare i dati personali necessari e non eccedenti per le finalità di cura dell'interessato
(esempio del dentista)
- anche a fronte delle finalità perseguite ed eventualmente per le quali si ha o meno raccolto un consenso

Accountability

Principi applicabili al trattamento dei dati personali

Esattezza:

- corretta individuazione del paziente c.f., calcolo automatico ATTENZIONE!!!
- configurazione corretta del fuso orario e sincronizzazione degli orologi con sistema NTP (Network Time Protocol) di tutti i dispositivi, anche per quei dispositivi off-line.
- Possibilità di esercitare i diritti applicabili (accesso, rettifica, cancellazione, limitazione, ..) da parte degli interessati attraverso i dati di contatto del titolare o del DPO.
- Segnalazione di eventuali errori, modifiche, o problematiche nella raccolta: qualora si ravvisi una inesattezza o ad esempio un indirizzo email risulti non corretto (perché viene segnalato un errore in automatico e/o nella mail di ritorno) si procede a correggere l'errore senza ritardo, ove necessario contattando gli interessati.
- Rifiuto di raccolta dei dati incompleti o imprecisi: qualora i dati siano incompleti o imprecisi e non permettano di effettuare le corrette attività di trattamento dati si procede a rifiutare l'acquisizione parziale o imprecisa, segnalando immediatamente la problematica all'interessato, o al soggetto che ha comunicato i dati.

Accountability

Principi applicabili al trattamento dei dati personali

Limitazione della conservazione:

- conservazione delle cartelle cliniche che, unitamente ai relativi referti, vanno conservate illimitatamente (Circolare del Ministero della Sanità del 19 dicembre 1986 n.900)
- documentazione iconografica radiologica, che deve essere conservata per un periodo non inferiore a dieci anni (art. 4, d.m. 14 febbraio 1997)
- nel caso in cui non sono disciplinati dalla normativa è il Titolare secondo il principio di responsabilizzazione ad individuare un periodo

Accountability

Principi applicabili al trattamento dei dati personali

Misure di sicurezza:

- Nomine ad incaricato (compiti e funzioni, obbligo di riservatezza, istruzioni, autorizzazione al trattamento) art. 29 GDPR, art. 2 quaterd. del Codice
- Formazione al personale
- Misure tecniche ed organizzative art. 32 GDPR + misure specifiche (Agid, Enisa, etc.)
- Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»)
- Misure tecniche ed organizzative previste da disposizioni di legge e provv. del Garante (es. FSE, DS, REF. ON LINE, «rispetto della dignità» 2005)
- Politiche per il trattamento dei dati e revisione periodica o all'occorrenza degli adempimenti (art. 24 GDPR)
- L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.
- Schema di certificazione ISDP@10003 «schema di processo e non di sistema»

Il Regolamento europeo in materia di protezione dei dati personali 2016/679

Monitoraggio continuo e aggiornamento

La conformità al Regolamento Europeo è un processo continuo. Le leggi e le interpretazioni normative possono mutare, così come la realtà delle organizzazioni ma anche le tecnologie. E' quindi fondamentale monitorare ed aggiornare le politiche e le prassi adottate