LE BUONE PRATICHE LEGATE AL TRATTAMENTO DEI DATI

L'Azienda Ospedaliero –Universitaria di Parma e il suo personale, devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, tenendo conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Ecco **alcune** delle principali buone pratiche da porre in essere durante il trattamento dei dati personali:

- **mantenere** l'assoluta **segretezza** e riservatezza, anche al termine del rapporto di lavoro o di collaborazione, sulle notizie e le informazioni di cui venga a conoscenza nell'ambito dell'attività svolta;
- **astenersi** dall'accedere a dati, informazioni, documentazione per finalità estranee alle proprie mansioni e attività lavorativa (es. consultazione di fascicoli o accesso a banche date informatiche per motivi personali…);
- **evitare** qualunque diffusione delle informazioni stesse, se non nei casi previsti dalla legge;
- **astenersi** dal rendere pubblico con qualunque mezzo, compresi il web o i social network, i blog o i forum, commenti, informazioni e/o foto/video/audio che possano ledere l'immagine dell'Azienda, l'onorabilità dei colleghi nonché la riservatezza o la dignità delle persone e in particolare dei pazienti;
- **custodire** gli archivi cartacei ed elettronici in modo da garantire la sicurezza dei dati in essi contenuti;
- **non fornire** per telefono le informazioni relative allo stato di salute di pazienti ricoverati; tutte le comunicazioni telefoniche devono avvenire in luogo riservato e possibilmente chiuso avendo cura di non trattare dati personali in presenza di terzi non autorizzati;
- **far rispettare** le appropriate distanze di cortesia e, per le prestazioni (sanitarie o amministrative) precedute da un periodo di attesa, **la chiamata** dell'utente **non deve** essere **nominativa;**
- mantenere riservate le proprie credenziali (ID E PSW) e **attenersi** alle indicazioni previste dal **Regolamento per l'utilizzo dei sistemi informatici**;
- la riproduzione di dati personali, in qualsiasi modo effettuata deve essere **limitata** ai casi di assoluta necessità, provvedendo, al termine dell'utilizzo, a che le copie cartacee e elettroniche siano distrutte o rese illeggibili e assicurandosi di **non riutilizzare** fogli contenenti dati personali;
- in caso di comunicazione dei dati personali ad uffici aziendali, occorre prestare **attenzione** a trasmettere **i soli dati necessari** alle finalità per cui sono stati richiesti.
- …

DOVE REPERIRE ULTERIORI INFORMAZIONI: Intranet aziendale (https://intranet.ao.pr.it/)→ Menù principale→ Direzione→ Settore Medico Legale →Privacy

REV_0 SETT_2018 REFRENTE PRIVACY

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Parma

IL REGOLAMENTO PRIVACY EUROPEO 2016/679/UE

Guida destinata ai professionisti dell'Azienda Ospedaliero Universitaria di Parma

Il Regolamento Europeo 2016/679 – **c.d. GDPR,** è il punto di arrivo di un percorso intrapreso dal Legislatore Europeo più di vent'anni fa. Risale infatti al 1995 l'approvazione della prima Direttiva Europea sulla protezione dei dati **(95/46/EC)** che viene recepita in Italia prima con la **L.675/1996** e poi con il **c.d. Codice Privacy (D.Lgs 196/2003)**. Tuttavia la flessibilità e l'elasticità di applicazione della Direttiva hanno fin da subito fatto emergere delle notevoli differenze tra i Paesi membri. Si rendeva quindi necessario approntare uno strumento, una fonte di maggiore forza, **il Regolamento Europeo**, che diversamente dalla Direttiva, una volta approvato è direttamente applicabile in tutti i Paesi. Dopo la piena applicabilità dal **25/05/2018** del Regolamento 2016/679 **c.d. GDPR**, l'Italia ha adottato un provvedimento, il **D.Lgs. 101/2018**, con l'intento di realizzare un'armonizzazione tra il Regolamento ed il precedente Codice Privacy.

Nel concreto, il GDPR ci lancia una sfida importante: il Legislatore ci invita a essere Garanti di noi stessi, soprattutto se ci troviamo a trattare dati relativi ad una sfera delicata e preziosa come quella della salute dell'individuo. Essere Garanti di se stessi significa soprattutto saper mettere in atto scelte su misura del trattamento effettivamente compiuto e saper rendere conto di tali scelte, mantenendo un livello di sicurezza non minimo, ma **ADEGUATO** al rischio legato al trattamento. **La sfida è lanciata ora tocca a noi!!**

GDPR e CODICE PRIVACY: COSA CAMBIA?

Cosa cambia con il GDPR:

1) L'approccio al trattamento dei dati personali che diventa *proattivo* (gestione dei dati fin dalla progettazione del servizio: **Privacy by design**);
2) La necessità di *minimizzare* i dati (limitare il trattamento ai soli dati strettamente necessari: **Privacy by default**);
3) La *responsabilizzazione* (cioè essere in grado di render conto delle proprie scelte in materia di trattamento dei dati: **Accountability**);
4) Introdotta la figura del *Responsabile della protezione dei dati* con funzioni di consulenza e collegamento con l'Autorità Garante (**RPD o DPO**);

Cosa non cambia:

1) Le *responsabilità* in capo ai **soggetti coinvolti** nel trattamento dei dati (che cambiano nome ma sono gli stessi: Titolare, Delegati, Autorizzati);
2) Le ***buone pratiche*** legate al trattamento dei dati;
3) La necessità di fornire delle "**Informazioni"** al paziente (prima Informativa) sulle modalità di trattamento dei dati.

LE DEFINIZIONI DEL GDPR

- ***«Dato personale»:*** *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») cioè la persona fisica che può essere identificata, direttamente o indirettamente;*
- ***«Interessato»:*** *è la persona fisica al quale si riferiscono i dati personali (es. l'utente, il fornitore…);*
- ***«Titolare del trattamento»:*** *la persona fisica o giuridica, l'autorità pubblica, che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;*
- ***«Delegato»:*** *il soggetto individuato dal Titolare che provvede all'ordinaria gestione del sistema, alla predisposizione di tutti gli aggiornamenti o precauzioni di natura tecnica, procedurale, organizzativa al fine di consentire il rispetto dei doveri di riservatezza.*
- ***«Autorizzato»:*** *colui che, dietro apposita autorizzazione, effettua materialmente le operazioni di trattamento sui dati personali (es. infermiere, operatore socio sanitario, medico, amministrativo….).*
- ***«Dati personali particolari»:*** *dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i 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;*
- ***«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.*

COSA SIGNIFICA TRATTARE I DATI?
il trattamento dei dati e i principi applicabili

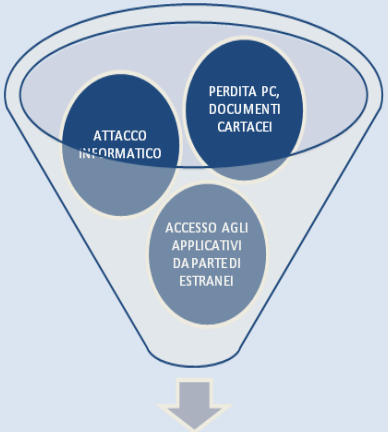
Il GDPR all'art. 4, definisce il trattamento dei dati come *"Qualsiasi operazione o insieme di operazioni, compiute* ***con o senza l'ausilio*** *di* ***processi automatizzati*** *e applicate a* ***dati personali*** *o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la 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."*

Ogni trattamento deve avvenire nel rispetto dei **principi** elencati dallo stesso codice:

1. **liceità, correttezza e trasparenza**;
2. **limitazione della finalità** (cioè definire delle finalità e poi trattarle i dati conformemente a esse)**;**
3. **minimizzazione dei dati** (cioè trattare solo i dati strettamente necessari);
4. **esattezza** (il che vuol anche dire aggiornamento);
5. **limitazione della conservazione** (solo per il tempo necessario per quella finalità);
6. **integrità e riservatezza**.

L'ERRATO TRATTAMENTO: LA VIOLAZIONE DEI DATI E LE SANZIONI

Il GDPR prevede anche il fenomeno della violazione dei dati (c.d. **DATA BREACH**) come: *"… ogni violazione della 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."*



DATA BREACH

LE SANZIONI

Le sanzioni previste in caso di mancato rispetto delle disposizioni sono di varia natura:

penale, civile, amministrativa, disciplinare.